JAMES M. WAGSTAFFE (95535)
MICHAEL VON LOEWENFELDT (178665)
MICHAEL NG (237915)
KERR & WAGSTAFFE LLP
101 Mission Street, 18th Floor
San Francisco, CA 94105
Tel.: 415-371-8500
Fax: 415-371-0500
Email: wagstaffe@kerrwagstaffe.com
Email: mvl@kerrwagstaffe.com
Email: mng@kerrwagstaffe.com

DAVID M. GIVEN (142375)
NICHOLAS A. CARLIN (112532)
PHILLIPS, ERLEWINE & GIVEN LLP
50 California Street, 32nd Floor
San Francisco, CA 94111
Tel: 415-398-0900
Fax: 415-398-0911
Email: dmg@phillaw.com
Email: nac@phillaw.com

Interim Co-Lead Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MARC OPPERMAN, et al.,

Plaintiffs,

v.

PATH, INC., et al.

Defendants.

Case No. 13-cv-00453-JST

CLASS ACTION

SECOND CONSOLIDATED AMENDED COMPLAINT

Hernandez v. Path, Inc., No. 12-cv-1515-JST
Pirozzi v. Apple Inc., No. 12-cv-1529-JST
Gutierrez v. Instagram, Inc., No. 12-cv-6550-JST
Espitia v. Hipster, Inc., No. 4:13-cv-432-JST
(collectively, the "Related Actions")

Plaintiffs Allen Beuershausen, Giuliana Biondi, Lauren Carter, Stephanie Cooley, Stephen Dean, Jason Green, Claire Hodgins, Gentry Hoffman, Rachelle King, Nirali Mandalaywala, Judy Paul, Maria Pirozzi, Theda Sandiford, Gregory Varner (collectively, "Plaintiffs") individually and on behalf of all others similarly situated, allege as follows:

INTRODUCTION

1. This case arises from the actions of Apple, Inc. ("Apple") and various developers of applications (the "App Defendants") created for use on three popular wireless mobile devices designed and sold by Apple: the iPhone, the iPad, and the iPod touch (collectively, the "iDevices"). The claims presented in this Second Consolidated Amended Complaint relate to three primary areas of liability.

2. First, Plaintiffs allege that with the assistance and cooperation of Apple, the App Defendants intentionally caused their Apps to secretly upload, store, and in some cases disseminate their personal and private address books as stored in the "Contacts" App from the iDevices without the knowledge or consent of the owners of the iDevices.

3. Second, Plaintiffs allege that Apple consciously and continuously misrepresented its iDevices as secure, and that the personal information contained on iDevices—including, specifically, address books—could not be taken without their owners' consent. Apple deliberately and widely disseminated that message by means of traditional marketing efforts, but also by means of "earned media" or a "buzz campaign," through which the company capitalized on its ubiquitous corporate presence and the immense public attention given anything Apple does. Through its deliberate statements that it knew would be broadcast worldwide by that vast network of traditional and non-traditional media, Apple created the false impression in the minds of the consumers that the iDevices were a safe and secure location for the storage of highly personal information like address book data.

4. Third, Plaintiffs allege that Apple had unique knowledge that its iDevices were not as secure as represented, but consistently and deliberately failed to reveal its products' security flaws to consumers, thereby continuing the false impression created by its partial statements. Apple not only failed to disclose that material information, which was in its

exclusive possession, but took active steps to conceal it. Plaintiffs allege that, as a result of Apple's conduct, Plaintiffs and millions of other people purchased iDevices reasonably believing that they were secure when, in fact, they are not, and then downloaded Apps, including the Apps manufactured by the App Defendants, and suffered the unexpected and unauthorized theft of their personal data.

5. Plaintiffs seek damages, injunctive relief, and disgorgement of the unjust enrichment and ill-gotten profits gained by defendants through their misconduct, as well as an injunction against Defendants' ongoing misconduct, including their use of wrongfully obtained address book data, among other relief.

JURISDICTION AND VENUE

6. This Court has original jurisdiction of this action under the Class Action Fairness Act of 2005. The amount-in-controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs, there are 100 or more class members, and there is minimal diversity because certain members of the class are citizens of a different state than any Defendant as required by 28 United States Code section 1332(d)(2).

7. This Court also has supplemental subject matter jurisdiction over Plaintiffs' related state law claims under 28 United States Code section 1367.

8. This Court has personal jurisdiction over Defendants. Each Defendant regularly conducts business in this judicial district and this action arose, at least in part, out of each Defendant's business in this judicial district. Each App Defendant (defined below) has done substantial business in California, with Apple, including appointing Apple as their agent to market and deploy the Apps to Plaintiffs' iDevices, which constitutes part of the conduct from which this action arose. The following Defendants are also headquartered within this federal judicial district: Apple, Inc., Electronic Arts, Inc., Foodspotting, Inc., Hipster, Inc., Instagram, LLC, Path, Inc., Twitter, Inc., and Yelp! Inc. All Defendants have sufficient minimum contacts with the United States, California, and this judicial district so that they are amenable to service of process, including under California's long-arm statute, and so that requiring them to respond to this action would not violate due process. This Court's jurisdiction over Defendants has been

confirmed in prior court rulings and/or by Defendants appearing without an objection to personal jurisdiction.

9. Venue is proper in this District under 28 United States Code section 1391(b) because each Defendants' improper conduct alleged in this Complaint occurred in, was directed from, and/or emanated from, in whole or in part, this judicial district. Additionally, the Court previously determined in its transfer order (Dkt. No. 217) that venue of this action is proper for all Defendants in the Northern District of California.

THE PARTIES

Plaintiffs

10. Plaintiff Lauren Carter is resident of the state of California.

11. Plaintiffs Allen Beuershausen, Claire Hodgins, Gentry Hoffman, Rachelle King, Nirali Mandaywala, Claire Moses, Judy Paul, and Greg Varner are residents of the state of Texas.

12. Plaintiff Giuliana Biondi is a resident of the state of Alabama. During the time of the conduct at issue in this case, she was a resident of the state of Texas.

13. Plaintiff Stephen Dean is a resident of the state of Illinois. During the time of the conduct at issue in this case, he was a resident of the state of Texas.

14. Plaintiff Stephanie Dennis-Cooley is a resident of the state of Virginia.

15. Plaintiff Jason Green is a resident of the state of Arkansas.

16. Plaintiff Maria Pirozzi is a resident of the state of New Jersey.

17. Plaintiff Theda Sandiford is a resident of the state of New York. During the time of the conduct at issue in this case, she was a resident of the state of Texas.

18. As described in more detail below, each Plaintiff purchased one or more iDevices after being exposed to Apple's continuous and deliberate media campaign concerning the security and safety of the iDevices, with the expectation that iDevices were secure (in particular, with respect to address book data), and that they either would not have purchased or would not have paid as much for those iDevices had the true facts concerning the insecurity of the iDevices been known to them. As further described in those paragraphs, many of the Plaintiffs

subsequently had personal information taken from their iDevices without their consent by one or more of the App Defendants.

Defendants

19. Defendant Apple, Inc. is a California corporation licensed to do business in California and throughout the United States. Its principal place of business is located in Cupertino, California. Apple has appeared in this action. At all relevant times, Apple designed, manufactured, promoted, marketed, distributed, and/or sold the Apple iDevices throughout the United States and California. Apple also sells Apps (including third party Apps) for iDevices in its App Store, and receives a portion of fees for Apps that it sells in the App Store. The App Store is operated from Apple's offices in the United States.

20. The following defendants are referred to collectively as the "App Defendants."

21. Defendant Chillingo Ltd. ("Chillingo") is a United Kingdom limited company with its principal place of business at Beechfield House, Winterton Way, Macclesfield, SK 11 OLP, United Kingdom.

22. Defendant Electronic Arts Inc. ("Electronic Arts") is a Delaware corporation with its principal place of business in Redwood City, California.

23. Defendant Foodspotting, Inc. ("Foodspotting") is a Delaware corporation with its principal place of business in San Francisco, California.

24. Defendant Foursquare Labs, Inc. ("Foursquare Labs") is a Delaware corporation with its principal place of business in New York, New York.

25. Defendant Gowalla Inc. ("Gowalla") is a Delaware corporation with its principal place of business in Austin, Texas.

26. Defendant Hipster, Inc. ("Hipster") is a Delaware corporation with its principal place of business in San Francisco, California. Hipster has already been served with process twice in the Opperman case through its registered Delaware agent for service of process, Agents and Corporations, Inc., 1201 Orange Street, Suite 600, One Commerce Center, Delaware 19801, but has not appeared and default has been entered against it on Opperman Plaintiffs' Second Amended Complaint. Dkt. Nos. 103, 346. Solely as against Hipster and in furtherance of that

entry of default and to pursue default judgment, Plaintiffs from the *Opperman* case maintain and expressly incorporate herein the allegations and claims of their Second Amended Complaint, Dkt. No. 103, against Hipster. The present document is not intended to amend Plaintiffs' action against Hipster.

27. Defendant Instagram, LLC ("Instagram") (originally named as Instagram, Inc.) is a Delaware limited liability company. On information and belief, Instagram's principal place of business is in San Francisco, California.

28. Defendant Kik Interactive, Inc. ("Kik Interactive") is a Canadian corporation with its principal place of business in Waterloo, Ontario, Canada. Kik Interactive has done substantial business in California, including with Apple since 2010. Plaintiffs' claims against Kik Interactive arise, in whole or in part, out of that business conducted by Kik Interactive in California, including the joint development with Apple of Kik Messenger (the Kik Interactive App at issue), and the marketing and distribution of Kik Messenger through the Apple App Store. Kik Interactive appointed Apple as its agent in connection with Kik Messenger, and Apple, operating from California in furtherance of that role, marketed Kik Messenger to Plaintiffs and deployed Kik Messenger on Plaintiffs' iDevices.

29. Defendant Path, Inc. ("Path") is a Delaware corporation with its principal place of business in San Francisco, California.

30. Defendant Rovio Entertainment, Ltd. s/h/a Rovio Mobile Oy ("Rovio") is a Finland corporation with its principal place of business in Espoo, Finland. Rovio has done substantial business in California, including with Apple since 2009. Plaintiffs' claims against Rovio arise, in whole or in part, out of that business conducted by Rovio in California, including the joint development with Apple of Angry Birds Classic (the Rovio App at issue), and the marketing and distribution of Angry Birds Classic through the Apple App Store. Rovio appointed Apple as its agent in connection with Angry Birds Classic, and Apple, operating from California in furtherance of that role, marketed Angry Birds Classic to Plaintiffs and deployed Angry Birds Classic on Plaintiffs' iDevices.

31. Defendant Twitter, Inc. ("Twitter") is a Delaware corporation with its principal place of business in San Francisco, California.

32. Defendant Yelp! Inc. ("Yelp") is a Delaware corporation with its principal place of business in San Francisco, California.

33. Defendant ZeptoLab UK Limited, also known as ZeptoLab ("ZeptoLab") is a United Kingdom limited company in London, United Kingdom. ZeptoLab has done substantial business in California, including with Apple since 2010. Plaintiffs' claims against ZeptoLab arise, in whole or in part, out of that business conducted by ZeptoLab in California, including the joint development with Apple of Cut the Rope (the ZeptoLab App at issue), and the marketing and distribution of Cut the Rope through the Apple App Store. ZeptoLab appointed Apple as its agent in connection with Cut the Rope, and Apple, operating from California in furtherance of that role, marketed Cut the Rope to Plaintiffs and deployed Cut the Rope on Plaintiffs' iDevices.

SUBSTANTIVE ALLEGATIONS[1]

Apple and its iDevices

34. Apple has the highest value of any corporation in the United States (nearly $480 billion), and is ranked fifth in the Forbes 500 with over $170 billion in annual revenue. A 2012 survey reported that half of all American households owned an Apple product, and Apple has over 41 percent of the United States market-share for smartphones. The Apple brand is one of the most recognizable in history. As discussed in more detail below, Apple's enormous scale and omnipresent role in American life means that every representation, promise, hint, or even rumor about Apple's products quickly spreads through traditional and non-traditional media to virtually the entire population of this country.

[1] Pursuant to the parties' Stipulation to Preserve Appellate Rights of Previously Asserted Claims, filed concurrently with this amended complaint, Plaintiffs have not replied certain claims and factual allegations related to those claims.

35. Since Apple launched the first iPhone in June 2007, iDevices have propelled the company's popularity and revenue, and have been a game-changer for Apple and the mobile device industry in general.

36. A similar revolution occurred with the iPad, a tablet based touch-screen computer whose impact on society and the computer industry was aptly summarized in the title of an online article published by businessinsider.com in 2013: "How the iPad Totally Changed The World In Just Three Years."

37. The iPod touch is a portable digital music and media player that utilizes Apple's proprietary iOS mobile operating system, and includes the ability to run most of the same Apps as an iPhone, essentially operating for purposes of this case as an iPhone without the phone capability.

38. iDevices come with a written limited warranty with a warranty period of one year from the date of purchase. Additional extended warranties were not available for purchase.

The App Store and Apple's Control Over App Development

39. In addition to their innovative hardware and operating system, iDevices' popularity and utility are driven by ready availability of mobile software applications ("Apps") for these iDevices. Apps are available exclusively from an Apple-controlled "App Store" which was launched in July 2008. Unlike most other manufacturers' mobile devices, iDevices run in a closed environment where third party software cannot be added except through the App Store. Apple has exclusive control over what Apps are available in the App Store, and the iDevices are designed to only accept software downloads from the App Store (thus, for example, clicking a link on a bank website for the bank's iPad App will take the consumer to the App Store; the bank cannot offer the software directly).

40. The App Store and the availability of numerous Apps to perform different functions are key parts of Apple's marketing strategy and the popularity of the iDevices. Since the launch of the App Store, Apple's Annual Report to shareholders has cautioned that "[t]he Company believes decisions by customers to purchase its hardware products depend in part on the availability of third-party software applications and services for the Company's

products…with respect to iOS devices, the Company relies on the continued availability and development of compelling and innovative software applications, which are distributed through a single distribution channel, the App Store."

41. Each iDevice comes pre-programmed with certain built-in Apps created by Apple. These Apple Apps cannot be deleted from the iDevice. Access to the App Store is provided through one of the built-in Apps and provides iDevice purchasers with instant access to any App available through the App Store. Another built-in Apps is the Contacts App as discussed further below.

42. Apple boasts approximately 700,000 Apps in the App Store for the iPhone/iPod Touch and around 275,000 Apps designed specifically for the iPad. Since July 2008, well over 40 billion Apps have been downloaded by customers using iDevices. The App Store generated $1.782 billion in revenues in 2010, $6.9 billion in 2011, and was on track to generate over $9 billion for calendar year 2012. While Apple shares App Store revenue with developers, it nevertheless profits from the Apps directly through sales and, more importantly, through the increased popularity of its iDevices. For example, Apple reported third-party App sales were one of the primary contributors to the $13.8 billion increase in Apple's net sales for its North American segment in 2011 along with the higher sales of the iPhone.

43. Apple prides itself on complete control over its products. Apple's former Chief Executive Officer ("CEO") Stephen Jobs publicly stated, "[O]ur job is to take responsibility for the complete user experience. And if it's not up to par, it's our fault, plain and simply."

44. To offer an application for download in the App Store, a third-party developer must be registered as an "Apple Developer," agree to the iOS Developer Program License Agreement with Apple, and pay a $99 yearly registration fee. Apple provides third-party developers with review guidelines, and conducts a review of all applications submitted for inclusion in the App Store for compliance with these documents. Developers are then licensed to use proprietary Apple software, code and tools—the same ones that Apple created and uses—to build iDevice Apps. Together, this Apple software (collectively known as the Apple iOS "Software Development Kit" or "SDK") and App Developer Program resources provide App

developers access to a wealth of information, tools, diagnostics and technical support services that Apple designed and published to facilitate and expedite the development of Apps for Apple's iDevices.

45. The resources Apple provides to these participants include editing software, simulators, forums, guides, design and approval criteria, code, code resources and libraries, APIs, performance enhancing tools, testing software, and mentoring via access to Apple engineers who "provide…code-level assistance, helpful guidance, [and] point [the developer] towards the appropriate technical documentation to fast-track [his/her] development process."

46. Thus, App developers do not start from scratch; Apple provides App developers all the pieces and components pre-built that they need to build iDevice Apps. As a result, all iDevice Apps were built, in part, by Apple.

47. The App Store Review Guidelines set forth the technical, design, and content guidelines Apple will use when reviewing an App for inclusion in Apple's App Store. These guidelines state that Apps "cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." In addition, Apple's requirements purport to require that Apps empower users to control access to user or device data, and require user consent before user or device data can be collected. Before allowing Apps into the App Store, Apple requires developers to submit their App and wait for approval or rejection by Apple (and rejected Apps are given feedback on the reason they were rejected so they can be modified and resubmitted). Apple has sole discretion over the App approval process and may reject a proposed App for any reason. Apple may further unilaterally choose to cease distributing any App at any time and for any reason. Apple has explicitly reserved the right to cease distributing any App that, among other things, (i) the App developer breaches the terms and conditions of the licensing agreements, (ii) the App developer provides Apple with inaccurate documents or information, or (iii) if Apple has been notified or has reason to believe that the App violates, misappropriates, or infringes the rights of a third party.

48. Apple also requires each App developer to re-submit his or her App for another round of testing and compliance verification whenever a change, update, or new version is built.

49. In addition to having exclusive control of the Apps offered for sale or download at the App Store, Apple controls the App development process. For example, App developers must buy and use Apple's Software Development Kit, which provides highly detailed guidelines for App development.

50. After Apple approves and provides a digital certificate for an App, Apple then markets, promotes, sells and deploys the App through the App Store, collecting all gross revenues and sales taxes. Apple retains 30 percent of the sale price of an App or any subsequent "digital goods" sold through an App, and 60 percent of any additional future revenues from Apps that incorporate Apple's iAd advertising program. Apple pays any applicable state sales tax for an App sale (for both itself and the App developer) based upon the stored account address it has for the recipient iDevice owner.

51. Apple contracts to serve as each App developer's agent for its App for these tasks.

52. Despite Apple's public statements that it protects its iDevice owners' privacy, Apple's App Developer Program tutorials and developer sites (which Apple does not make available to consumers) teach App developers just the opposite—how to code and build Apps that non-consensually access, use and upload the mobile address books maintained on Apple iDevices—precisely what these App Defendants' identified Apps did. As App developers, the App Defendants were exposed to and aware of these tutorials and developer sites and, on information and belief, their personnel utilized them to build the identified Apps.

53. Apple thus completely controls owners' experience from development of the iDevice, development and selection of the Apps available at the App Store, as well as restriction of how the iDevice can be modified by owners (*e.g.*, such as blocking owners from modifying their devices or installing unapproved software on their Apple Devices). Through the iOS Developer Program License Agreement, Apple further restricts information concerning the development process and prohibits developers from publicly discussing Apple's standards for App development.

Contacts on the iDevices

54. As discussed above, each iDevice comes pre-loaded with, among other things, an Apple "Contacts" App. The Contacts App allows iDevice owners to customize address books using the following fields: (1) first and last name and phonetic spelling of each, (2) nickname, (3) company, job title and department, (4) address(es), (5) phone number(s), (6) e-mail address(es), (7) instant messenger contact, (8) photo, (9) birthday, (10) related people, (11) homepage, (12) notes, (13) ringtone, and (14) text tone.

55. When the owner first receives the iDevice, all of the fields for the Contacts App address book are blank. To utilize the Contacts App, the owner must individually input entries for each of the address book fields, using the touch screen key pad on the iDevice, or they can import contacts that they created on their computer. Address book data can be synced with a computer or cloud-based data sources.

56. In the recent words of the United States Supreme Court, "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" Riley v. California, 573 U.S. ___ (2014) (citations omitted). The information in the Contacts App is among the most private and personal of such information a user maintains on an iDevice. The address book data reflects the connections, associations, and relationships that are unique to the owner of the iDevice. The information stored therein, as well as the manner in which it is stored, is highly personal and private. Address book data is not shared, is not publicly available, is not publicly accessible, and is not ordinarily obtainable by a third party unless the owner physically relinquishes custody of his or her iDevice to another individual.

57. Most consumers are highly concerned about the privacy of their address book data. In a survey reported by the Berkeley Center for Law & Technology at the UC Berkeley School of Law published in July 2012, 81 percent of respondents said they would either probably or definitely not allow a social networking App to collect their contact list to suggest more friends, and 93 percent said they would probably or definitely not allow a coupon App to collect their contact list to send coupons to their contacts.

58. In addition to being highly private, the address book data has independent value, both reflecting the effort required for the individual user to compile the data, and also its commercial value to third parties.

59. Contact data is of particular commercial value to businesses engaged in profiting from and exploiting social media, including through advertising. Even mere lists of addresses, phone numbers, and email addresses are by themselves commodities available for sale in the marketplace, but data reflecting the real-world social connections between people is of the highest value, and has driven the titanic success of Facebook and others.

60. Address book data is exactly that type of richly valuable information. By taking Plaintiff and other class members' address book data, Defendants acquired a road map to users' personal lives, and were able to exploit that wrongfully obtained valuable data to grow of their businesses.

Apple's Ubiquitous Media Presence and the Wide Dissemination of Its Statements

61. Apple engaged in a long-term, widely distributed marketing campaign to convince potential customers that Apple iDevices were safe and secure, and that they protected consumers' privacy.

62. Apple's marketing campaign included traditional and non-traditional methods. Apple was well aware that everything said by its CEO, Stephen Jobs, and other top executives, especially involving Apple's policies and new products or versions, would be eagerly followed by the media and the public. Such statements were invariably reported by thousands of media outlets, dissected by pundits and bloggers, frequently posted on Apple's own website, and available on countless websites and social media platforms, and thus made available to virtually all potential customers.

63. Apple intentionally used this type of marketing campaign, sometimes referred to as "earned media" or "buzz marketing," as a major part of its marketing and advertising strategy, and as an adjunct to its traditional paid advertising. Apple even employed a "Worldwide Global Director of Buzz Marketing" who worked on all the iPhone product launches.

64. According to data released by Dow Jones, Apple was mentioned approximately 89,222 times in English global print publications in 2010 and up to 130,511 times in 2011. Similarly, data shows that Apple product releases are widely reported. For example, when the new iPad was announced in January 2010, there was over 5.2 million posts on social networking sites, 70,796 news articles, 199,979 forum posts, and 246,866 blog entries within a one-month period. Adding to the reporting frenzy are the over one million third-party Apple developers who are invested in promoting and publicizing Apple buzz statements and marketing efforts to consumers.

65. A Nielsen study in 2013 found that "earned" media is the most trusted source of information in all countries it surveyed worldwide. It also found that earned media is the channel most likely to stimulate the consumer to action.

66. Apple also uses its website to feed the buzz, as well as to provide information directly to the public (including individuals who seek out additional information as a result of Apple's publicity campaigns). Surveys show that Apple's website is one of the most visible and highly trafficked in the world (with roughly 80 million unique visitors per month), and that consumers spend a good deal of time on Apple's websites (usually around 1¼ hours). In 2008, Apple's website, Apple.com, was the fifth most-visited retail site on Cyber Monday, the online shopping day after the Thanksgiving holiday weekend sales. By 2010, Apple's website ranked second among online retailers. And by 2011, Apple had more online visitors to its website than Walmart and rivaled that of the New York Times.

67. Apple uses other technologies to communicate directly to consumers, including "Hot News" (a compilation of Apple announcements published by the company) and an RSS news stream. Consumers can sign up for these services and receive "news" articles and press releases by Apple and about Apple's statements, advertisements, and product launches. These services also promote and disseminate statements made by Apple representatives at technology conferences. On information and belief, a large number of consumers and media outlets subscribe to those services.

68. Apple also utilizes informal but strategic leaks, as well as formal press releases to publicize its products and deliver its marketing message to consumers.

69. According to Apple's Director for the App Store, Matthew Fischer, Apple relied on traditional media, Apple's website, third-party websites, promotional emails, in Apple's own brick-and-mortar retail stores, as well as unsolicited media coverage in the United States and worldwide to advertise the launch of the App Store. Since launching the App Store on July 10, 2008, Apple has spent hundreds of millions of dollars on advertising the App Store. Apple also touts the App Store as a key feature of its iDevices, for example in its widely disseminated traditional print and television commercials, Apple emphasizes to consumers that "if you don't have an iPhone, you don't have the App Store, so you don't have the world's largest selection of apps that are this easy to find and this easy to download right to your phone…."

70. As Apple was creating the App Store and subsequent App market, Apple was also ramping up its security settings for the next iteration of the iPhone (the iPhone 3G launched in July 2008). Apple's efforts were aimed at creating widespread acceptance of the iPhone for corporate use. As such, Apple aggressively marketed the iPhone as safe and secure for corporate applications.

71. Apple communicated its message of safety in other ways as well, including through its product literature and even on its receipts. For example, as Apple launched its marketing effort for the iPhone 3G, Apple's privacy policy began using the phrase, "Your privacy is a priority at Apple, and we go to great lengths to protect it." Apple has continuously used this phrase and/or similar variations to expound its commitment to its customers' security.

72. Around 2010, Apple launched another marketing effort to demonstrate to customers that it valued and protected their privacy. Like numerous prior product marketing efforts, Apple purposely leaked information to amplify its media attention. In addition to the "earned media" campaign, Apple also publicized its commitment to privacy by testifying before the United States Senate. These efforts were part of Apple's campaign to convince consumers that it is a trustworthy company that protected consumers' privacy.

73. Apple's marketing campaign was successful in convincing a large number of consumers that it could be trusted for protecting consumer privacy. For example, a 2009 consumer survey conducted by the Ponemon Institute ranked Apple eighth among all companies as "most trusted for privacy." In 2010, Apple ranked twelfth, in 2011 it ranked fourteenth, but in 2012, after the damaging revelations of various privacy violations, such as the one at issue in this case, it fell out of the top twenty.

74. Thus, since at least the inception of the iPhone in 2007 and up to the filing of this lawsuit, Apple has meticulously disseminated its privacy and security message to the public through traditional and non-traditional marketing efforts, with a particular emphasis on "earned media" and "buzz marketing," and a robust online presence through its website.

75. Apple's marketing campaign, the contents of which are described in greater detail below, has been widely disseminated through both traditional and non-traditional means, including channels Apple is uniquely positioned to exploit. In short, nothing Apple says goes unnoticed, but is repeatedly broadcast to a highly interested public audience worldwide.

Apple's Marketing of iDevices As Private and Secure

76. Apple's focus on privacy has been a cornerstone of its marketing strategy for the iPhone (and later iDevices) as well as for Apps. Since the first iPhone, Apple has claimed that it acts with the goal of protecting the customers' privacy and repeatedly marketed Apple's products as "safe" and "secure," pervasive themes running through Apple's traditional and non-traditional marketing efforts. The following are examples of the publicized representations that Apple has made regarding the safety, security, and privacy of Apple's iDevices, the address books as stored on these iDevices, and the iOS system (the operating system that runs on iDevices):

i) On January 9, 2007, at the unveiling of the iPhone, Apple's CEO Stephen Jobs stated that Apple chose to use the iOS operating system on the iPhone because "it's got everything we need…***We've been doing this on mobile computers for years. It's got awesome security***…It's got all the stuff we want…Not the crippled stuff that find on most phones. This is real, desktop-class applications." (Ex. A (emphasis added).) Video clips

of this presentation as posted on YouTube.com have generated well-over one million views. Furthermore, these statements were made at the Apple MacWorld 2007 conference and were widely publicized and disseminated through the mainstream and non-traditional media.

ii) The April 10, 2007 Apple Customer Privacy Policy as available on the Apple website stated, "***Apple takes precautions***—including administrative, technical, and physical measures—***to safeguard your personal information*** against loss, theft, and misuse, as well as unauthorized access, disclosure, alteration, and destruction." (Ex. B (emphasis added).) These representations and similar variations, such as "Apple takes the security of your personal information very seriously" have been continuously available on Apple's Apple Store website. This statement was widely publicized and disseminated through the mainstream and non-traditional media.

iii) On May 30, 2007 at the D5 conference, *i.e.* All Things Digital Conference, hosted by the Wall Street Journal, Mr. Jobs stated in response to a question as to whether the iPhone will be opened up to App developers in the future, "This is a very important tradeoff between security and openness, right, and what we want is we want both. We want to have our cake and eat it too." He also said, "Until we find that way, ***we can't compromise the security of the phone***." (Ex. C (emphasis added).) As the sponsor, the Wall Street Journal covered the conference in a worldwide report. In addition, other mainstream and non-traditional media widely publicized the conference. This statement was widely publicized and disseminated through the mainstream and non-traditional media.

iv) During the keynote presentation at the June 11, 2007 Apple Worldwide Developer Conference ("WWDC"), Mr. Jobs claimed that Apple had

innovated a way to "let[] developers write great apps and yet ***keep the iPhone reliable and secure***." Mr. Jobs emphasized that Apple had selected Web 2.0 apps that would be "***sandboxed*** on the iPhone," meaning "they ***run securely on the iPhone so they don't compromise its security or reliability***." "[T]hey're secure, with the same sort of security you'd use for transactions with Amazon or a bank," he explained to the crowd.

In a follow-up press release titled *iPhone to Support Third-Party Wed 2.0 Applications*, also issued in connection with the WWDC on June 11, 2007, by Apple representative Stephen Dowling, Apple stated, "Third-party applications created using Web 2.0 standards can extend iPhone's capabilities without compromising its reliability or security...Our innovative approach, using Web 2.0-based standards, lets developers create amazing new applications while keeping the ***iPhone secure and reliable***." (Ex. D (emphasis added).) The described statements in Mr. Jobs' keynote regarding iPhone security and this press release were both widely disseminated and publicized in the news media, and via online reports and blogs, with numerous media outlets covering the keynote in real time and live-blogging it to the online versions of their news sites. Apple also immediately posted a video of Mr. Jobs' keynote on its website, made it available to consumers via a QuickTime video-on-demand, and kept it posted and available for several years. The keynote video has also been posted to YouTube, where it remains posted and available and has received over 500,000 views. Further, Apple directly disseminated this statement to consumers and interested media through its Hot News service and RSS news feed. This statement was widely publicized and disseminated through the mainstream and non-traditional media. As with all of Apple's press releases, the press release was posted to its website and remained available there.

v) On or about October 18, 2007, Apple posted an open letter, again from Mr. Jobs, on its website regarding its decision to delay allowing outside App developers to create and run Apps on the iPhone. The letter explained that Apple intended to wait to roll out the software development package for App developers until it could ensure that it could "***protect iPhone users*** from viruses, malware, privacy attacks, etc." (Ex. E (emphasis added).) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

vi) On or about March 6, 2008, at an event promoting the App Store, Mr. Jobs stated, "You [the consumer] don't have to worry about 3rd party Apps mucking it up. On the other side you've got a Windows PC where people spend a lot of time every day making it usable. ***We want to take the best of both: reliability of the iPod, but the ability to run 3rd party Apps***. They get an electronic certificate... if they write a malicious app we can track them down and tell their parents...We define the software on the phone, we run the dev program, we distribute the Apps! This is our program, and we're running it." He further stated, "Now, will there be some limitations? Of course. ***There are going to be some Apps that we're not going to distribute***. Porn, malicious Apps, ***Apps that invade your privacy***. ***So there will be some Apps that we're going to say no to***…." (Ex. F (emphasis added).) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

vii) Beginning on or about July 11, 2008, upon Apple's launch of the iPhone 3G, Apple's product page explained why the iPhone was the "best phone for business. Ever." The webpage stated that the iPhone "delivers ***secure access*** to corporate intranets" and corporate resources, and "companies can ***securely sync***." (Ex. G (emphasis added).) These statements were part of Apple's concentrated marketing strategy and efforts to sell the

iPhone to business-users. This statement was widely publicized and disseminated through the mainstream and non-traditional media.

viii) On or around July 20, 2008, as available on the Apple website, Apple's privacy policy began using the phrase "***Your privacy is a priority at Apple, and we go to great lengths to protect it***." (Ex. H (emphasis added).) Apple continuously used this phrase and/or variations of it (*i.e.* "Your privacy is important to Apple.") in all subsequent iterations of its privacy policy. This statement was widely publicized and disseminated through the mainstream and non-traditional media.

ix) On or around August 28, 2008, in an article, *Apple Working on iPhone Software Update to Fix Security Flaw*, Apple issued a statement that it was "readying a software update to the iPhone, fixing a security flaw in the device ***that gives unauthorized access to contacts and e-mails***." In the article, Apple spokeswoman Jennifer Bowcock said, "We are aware of this bug." This article was widely publicized and disseminated through the mainstream and non-traditional media.

x) Since 2009, Apple's "iPhone User Guide for iPhone OS 3.1 Software," and on information and belief subsequent versions of the same, which were publicly available on the Apple website, stated that the iPhone's security features "protect the information on the iPhone from being accessed by others." (Ex. I.)

xi) The March 17, 2009 version of Apple's iOS Developer Program License Agreement stated: "Any form of user or device data collection…must comply with all applicable privacy laws and regulations as well as any Apple program requirements related to such aspects, including but not limited to any notice or consent requirements." (Ex. J.) Apple continuously used this phrase and/or variations of it in all subsequent iterations of its Developer Program License Agreement. This statement

was widely publicized and disseminated through the mainstream and non-traditional media.

xii) On or around June 1, 2009, Apple's product description, *iPhone in Business – Security Overview*, as available on the Apple website, stated, "[an] ***iPhone can securely access corporate services and protect data on the device***. It provides strong encryption for data in transmission, proven authentication methods for access to corporate services, and for iPhone 3GS, hardware encryption for all data stored on the device." (Ex. K (emphasis added).) These statements were part of Apple's concentrated marketing strategy to sell the iPhone to business-users. This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xiii) On or around June 19, 2009, after the launch of the new iPhone 3G, Apple's webpage advertised the iPhone's security features as making "each ***iPhone secure and ready for business***[.]" (Ex. L (emphasis added).) The iPhone 3G incorporated Microsoft Exchange, along with a host of other pro-business updates, which was advertised as enabling a company's IT administrators to "***securely manage any iPhone***[.]" (Ex. L (emphasis added).) These statements were part of Apple's concentrated marketing strategy to sell the iPhone to business-users. This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xiv) In a November 22, 2009 article, *Apple's Schiller Defends iPhone App Approval Process*, published by the widely distributed Bloomberg Businessweek, Apple's senior vice president for worldwide product marketing, Phil Schiller, stated, "[Apple has] built a store for the most part that ***people can trust***," and that "We [(Apple)] review the applications to make sure they work as the customers expect them to work when they

download them." In discussing Apps that were not approved, Schiller said, "There have been applications submitted for approval ***that will steal personal data***, or which are intended to help the user break the law, or which contain inappropriate content." (Ex. M (emphasis added).) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xv) In an April 8, 2010 Apple press release, *Apple Previews iPhone 4 OS*, by Apple representative Trudy Muller, Apple stated that the operating system provides "enhanced Enterprise support with ***even better data protection***, …New enterprise features in iPhone OS 4 include ***improvements in security***,…The ***new Data Protection feature***….iPhone OS 4 now provides the option to set longer, more complex passcode, ***making the iPhone and its data even more secure***." (Ex. N (emphasis added).) Apple directly disseminated this statement to consumers and interested media through its Hot News service and RSS news feed. All of Apple's press releases are posted to its website and remain available there. This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xvi) In a May 2010 email correspondence to Valleywag website editor Ryan Tate, Mr. Jobs stated that the App Store provides "***freedom from programs that steal your private data***. Freedom from programs that trash your battery. Freedom from porn. Yep, freedom. The times they are a changin', and some traditional PC folks feel like their world is slipping away. It is [.]" (Ex. O (emphasis added).) This email and statement were widely publicized and disseminated through the mainstream and non-traditional media.

xvii) On June 1, 2010, at the D8 Conference, or the All Things Digital Conference, hosted by the Wall Street Journal, Mr. Jobs stated, "***We take***

privacy extremely seriously...That's one of the reasons we have the curated Apps store. We have rejected a lot of Apps that want to take a lot of your personal data and suck it up into the cloud…." (Ex. P (emphasis added).) He also stated, ***"[P]rivacy means people know what they're signing up for, in plain English, and repeatedly.*** That's what it means. … And some people want to share more data than other people do. ***Ask 'em. Ask 'em every time.*** Make them tell you to stop asking them if they get tired of your asking them. ***Let them know precisely what you're going to do with their data.*** That's what we think." As the sponsor, the Wall Street Journal covered the conference and publicized Mr. Jobs' statements. In addition, other mainstream and non-traditional media outlets widely publicized the conference.

xviii) On or around June 7, 2010 at Apple's World Wide Developer Conference in San Francisco, California, Mr. Jobs announced that Apple's products, including iDevices, will have "[e]ven better ***data protection***[.]" (Ex. Q.) The Conference has been hosted by Apple since the 1990s. The 2010 Conference was particularly popular, Apple sold out of the 5,000 tickets (priced at $1,599 each) within twelve hours. The Conference was widely reported by mainstream and non-traditional media and reached consumers, some of whom posted online comments regarding Apple's presentations and products.

xix) In a June 7, 2010 article, *Recap: Apple Announces New iPhone*, as published by the Wall Street Journal regarding Apple's World Wide Developer Conference, Mr. Jobs was quoted as calling the App Store a "curated platform" because it is "the most vibrant app store on the planet." (Ex. R.) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xx) Since July 2010, Apple's website consistently represented the iPhone as "***Safe and secure by design***. iOS 4 [the iPhone operating system] is ***highly secure*** from the moment you turn on your iPhone. ***All Apps run in a safe environment***, so a website or app can't access data from other Apps. iOS 4 supports encrypted network communication to protect your sensitive information...." For example, with the release of Apple's iOS 4 software, Apple touted: "iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can't access data from other apps. iOS 4 supports encrypted network communication to protect your sensitive information. Optional parental controls let you manage iTunes purchases, Internet browsing, and access to explicit material. To guard your privacy, apps requesting location information must get your permission first. You can set a passcode lock to prevent unauthorized access to your phone and configure iPhone to delete all your data after too many unsuccessful passcode attempts." This message was substantially repeated at all relevant times. In September 2012, Apple extended the safety message to all devices and provided on its website that "iOS is highly secure from the moment you turn on your device. All apps run in a safe environment, so a website or app can't access data from other apps. iOS also supports encrypted network communication to protect your sensitive information. To guard your privacy, apps requesting location information are required to get your permission first. You can set a passcode lock to prevent unauthorized access to your device and configure it to delete all your data after too many unsuccessful passcode attempts." This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xxi) On or around September 9, 2010, Apple published the App Store Guidelines on the Apple website, which stated, "Developers that attempt to reverse lookup, trace, relate, associate, mine, harvest, or otherwise exploit Player IDs, alias, or other information obtained through the Game Center will be removed from the iOS Developer Program." (Ex. S.) The Guidelines also stated, "***Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used***. Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected." Since this version, the Guidelines have continuously represented that Apple will reject Apps that transmit data without consent or remove private user data. These guidelines were publically posted on Apple's website. To further promote dissemination of the Guidelines to consumers, Apple linked this webpage to other webpages on its website to promote its claim that Apps were reliable, performed as expected, and were free from material that take users' data. This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xxii) On or before September 9, 2010, Apple's 2010 License Agreement Update stated that "You [(App developers)] and ***Your Applications may not collect user or device data without prior user consent***, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising. You may not use analytics software in Your Application to collect and send device data to a third party." This statement was widely publicized and disseminated through the mainstream and non-traditional media. For example, this was discussed in an article, *A Taste of What's New in the Updated App Store License Agreement*, by John Gruber. (Ex. T (emphasis added).)

xxiii) In a December 17, 2010 article, *Your Apps Are Watching You*, by Scott Thurm and Yukari Iwatani Kane of the Wall Street Journal, Apple spokesman Tom Neumayar was quoted as stating: "We have created ***strong privacy protections for our customers . . . Privacy and trust are vitally important.***" Mr. Neumayar further stated that iPhone Apps "***cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used.***" (Ex. U (emphasis added).) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xxiv) Starting at least as early as January 1, 2011, Apple's official electronic receipts from Apple's App Store stated, "***Apple respects your privacy***" across the bottom. On information and belief, billions of such receipts have been distributed.

xxv) In a February 15, 2011 Apple press release, *Apple Launches Subscriptions on the App Store*, by Apple representative Trudy Miller, Apple stated that "***Protecting customer privacy is a key feature*** of all App Store transactions." (Ex. V (emphasis added).) Apple directly disseminated this statement to consumers and interested media through its Hot News service and RSS news feed. All of Apple's press releases are posted to its website and remain available there. This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xxvi) At or around the same time, after Apple's launch of the App subscription service from the App Store, Apple's website regarding the service stated, "Protecting ***customer privacy is a key feature*** of all App Store transactions." This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xxvii) In an April 27, 2011 article, *Apple Responds To Location Log Scrutiny With Extensive Q&A Response*, by Graham Spencer, Apple was asked, "Does Apple believe that personal information security and privacy are important?" Apple responded, "Yes, we strongly do. For example, iPhone was the first to ask users to give their permission for each and every app that wanted to use location. ***Apple will continue to be one of the leaders in strengthening personal information security and privacy***." Apple further stated that it is leading the way when it comes to privacy. (Ex. W (emphasis added).) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xxviii) In the July 5, 2011 version of the Apple Developer Agreement, Apple stated, "You and Your Application ***may not collect user or device data without prior user consent***, an then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising. You may not use analytics software in Your Application to collect and send device data to a third party." (Ex. X (emphasis added).) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

xxix) In a February 15, 2012 article, *There's an Easy Fix to Apple's Latest iPhone Privacy Problem*, by Rebecca Greenfield for the Atlantic Wire, Mr. Jobs is quoted as having said, in regards to users' privacy, "Ask them. Ask them every time. Make them tell you to stop asking if they get tired of you asking. Let them know precisely what you are going to do with their data." (Ex. Y.) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

77. In addition to these more general representations regarding the security and privacy of iDevices, Apple went further by publicizing the iDevices' specific security features. In particular, Apple made repeated statements regarding the "sandboxing" security feature,

which compartmentalizes the Apps and their related data sets from each other. Apple represented that "sandboxing" protected and secured the owners' iDevices—for example, preventing address book data stored in the Contacts App from being accessed by other, third-party Apps. Specifically, Apple made the following additional representations regarding sandboxing:

i) In a 2008 videotaped question and answer session after the introduction of the App Store, an Apple representative stated that Apple is "putting . . . a number of different things in place, from ***sandboxing to other . . . technical things you want to do to protect applications and the [iPhone] system***." Mr. Jobs, also stated that "…we think we've put in good safeguards where, if we miss something, we'll be alerted to it real fast by users, and we'll just turn off the spigot so no more users have problem[.]" This statement was widely publicized and disseminated through the mainstream and non-traditional media.

ii) In a 2010 scholarly article, *iPhone Privacy*, by Nicolas Seriot, an Apple representative stated, "***Applications on the device are 'sandboxed' so they cannot access data stored by other applications***. In addition, system files, resources, and the kernel are shielded from the user's application space." (Ex. Z (emphasis added).)

iii) In a February 23, 2011 statement at Apple's annual shareholder meeting, Apple's iOS development leader, Mr. Forstall, explained that the iOS was secure by mentioning its sandbox design that prevents viruses or malware from "stealing contacts." He further stated that "sandboxing" provides iDevice security and prevents Apps from stealing contacts. This statement was distributed widely on the internet by appleinsider.com among other websites and media outlets. (Ex. AA.)

iv) In an April 27, 2011 article, *Stephen Jobs Discusses Location Tracking, Privacy*, by Federico Viticci for MacStories, Mr. Jobs, explained that the

system on iDevices "had ***root protection and was sandboxed*** from any other application[.]" (Ex. BB.) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

v) In a June 18, 2011 article, *Security Through Sandboxing-Towards More Secure Smartphone Platforms*, by the Center for Computing Technologies, Apple stated, "***Applications on the device are 'sandboxed'*** so they cannot access data stored by other applications." Apple's head of iTunes, Greg Joswaik, was quoted for stating, "Why do we have these security mechanisms in [the iPhone]? ..[W]e want to secure the user's data. Again, their E-mail, their contacts [sic], their pictures, et cetera." (Ex. CC (emphasis added).) This statement was widely publicized and disseminated through the mainstream and non-traditional media.

78. In addition, Apple has repeatedly publicly stated that it has intentionally cultivated consumer confidence that Apple is protecting its customer's private data, and in particular that Apple does not allow access to data stored on customers' iDevices without prior notice and clear consent. Those public admissions include the following examples:

i) In an August 21, 2009 article, Apple Answers the FCC's Questions, Apple stated, "We created an approval process that reviews every application submitted to Apple for the App Store in order to ***protect consumer privacy***, safeguard children from inappropriate content, and avoid applications that degrade the core experience of the iPhone[.]"

ii) In a July 12, 2010 letter to United States Representatives Markey and Barton, *Apple Inc.'s Response to Request for Information Regarding its Privacy Policy and Location Based Services*, by Apple's general counsel and senior vice president of legal and government affairs, Bruce Sewell, Apple stated: "Apple is ***committed to*** giving its customers ***clear notice and control over their information***, and we believe our products do this in a simple and elegant way."

iii) On July 27, 2010 before the United States Senate, Apple's vice president for software technology, Dr. Guy Tribble, repeated these themes in widely reported testimony: "Apple shares your [(the Senate's)] concerns about privacy, and we remain ***deeply committed to protecting the privacy of our customers*** through a comprehensive approach implemented throughout the company. We're committed to providing our customers with clear notice, choice, and control over their information."

iv) In an April 12, 2011 sworn declaration, Apple's director for the App Store, Matthew Fischer, stated that Apple's "App Store name has a robust presence throughout the United States[.]…Apple has taken rigorous steps to ensure that software available from the service [*i.e.* Apps] does not include inappropriate content, viruses, or malware. Apple has invested in these screening measures because it views them as essential to building and maintaining ***a public reputation for providing a service that offers safe, secure software that protects the integrity, performance, and stability of users' mobile devices***." Fischer further explained that Apple built this robust presence and public understanding through traditional media, Apple's website, third-party websites, promotional emails, in Apple's own brick-and-mortar retail stores, as well as through unsolicited media coverage in the United States and worldwide.

v) In May 10, 2011 written testimony of Dr. Tribble stated: "***Apple is deeply committed to protecting the privacy of our customers*** who use Apple mobile devices, including iPhone, iPad and iPod touch. Apple has adopted a comprehensive privacy policy for all its products and implemented industry-leading privacy features in its products to protect our customers' personal data." Dr. Tribble further testified: "We do not share personally identifiable information with third parties for their marketing purposes without consent, and we require third-party application developers to

agree to specific restrictions protecting our customers' privacy. ***Apple is constantly innovating new technology, features and designs to provide our customers with greater privacy protection and the best possible user experience***." He also testified: "Apple is strongly committed to protecting our customers' privacy. We give our customers clear notice of our privacy policies, and our mobile products enable our customers to exercise control over their personal information in a simple and elegant way."

vi) During an appearance in May 2011, before the United States Senate, Dr. Tribble testified that Apple goes beyond stated privacy policies to inform users of the use of their private information. Dr. Tribble also testified that Apple will "yank" Apps that are collecting private user data without users consent.

Apple's Undisclosed Knowledge That Private Data On The iDevices Is, In Fact, Not Secure

79. Contrary to the repeated assurances Apple has provided to the public, Apple-approved Apps have repeatedly accessed, downloaded and copied owners' private address books without the owners' knowledge or consent.

80. In early February 2012, it was discovered that the Path App was uploading data stored on owners' iDevices (including address books and calendars) to its servers. The discovery of this data breach, which Apple had led the public to believe was impossible, was followed by a public admission and apology by Path's Chief Executive Officer.

81. The public revealing of these data thefts led to several Congressional inquiries and newspaper articles. At all times Apple contended that it had done nothing wrong and that it took necessary steps to protect consumers' private information.

82. However, while the Path's disclosures were the first well-known public examples of data theft by Apps, Apple was long aware that the address books were not actually secure.

83. In 2008, just a few weeks after the launch of the App Store, Apple approved and released the Aurora Feint App to the App Store, where it was downloaded and installed on hundreds of thousands of consumers' iDevices. Apple later removed the App when it was revealed to be transmitting iDevice owners' address books to the developer's servers without asking if it could do so. After a three-day ban from the App Store, it returned with Apple's approval (but this time missing the malicious portion that caused Apple to pull it). Apple again promoted the re-released Aurora Feint App on its "What We're Playing App Store" list despite the developer having just flouted Apple's policies and violated consumers' privacy.

84. The next year, four months after releasing the Google Voice App to the App Store and downloading and deploying the App to a substantial number of consumers' iDevices, Apple delisted that App. When questioned by the FCC about the removal of its competitor's App, Apple admitted that "the iPhone user's entire Contacts database is transferred to Google's servers, and we [Apple] have yet to obtain any assurances from Google that this data will only be used in appropriate ways."

85. Despite this clear knowledge that its prior and ongoing representations were false and misleading, Apple never disclosed to the public, including Plaintiffs, that iDevices could transmit the address books without owner input or authorization, that the "Contacts" feature and its address books were not sandboxed and lacked promised security protections, or that Apple had experienced repeated instances of Apps exploiting these security flaws.

86. To the contrary, Apple led consumers to believe that it timely addressed all vulnerabilities to keep the iDevices safe and secure. For example, on July 31, 2009, Apple made an iOS software upgrade available to fix a software vulnerability. Apple's spokesman said that the upgrade was offered less than 24-hours after Apple was alerted to the vulnerability. He assured consumers that "no one [was] able to take control of the iPhone to gain access to personal information using this exploit."

87. Apple actively concealed its failure to correct the security problem and the ability of Apps to access users' address book data without consent. For example, Apple removed BitDefender's Clueful, an App designed to inform its users of whether other Apps were stealing

their address books among other data. Apple also imposed a one-year ban on security researcher Charlie Miller when in late 2011, he intentionally passed a non-compliant App through Apple's review and onto the App Store in a proof-of-concept security test and reported to Apple the gaping security hole that he found in Apple's App procedures. Apple thus not only failed to reveal the iDevices' lack of security, it sought to prevent consumers from learning those facts and punished those who revealed them.

88. Even worse, despite its purported policies preventing data theft, Apple contractually required App developers to abide by its *iOS Human Interface Guidelines* reference manual included in Apple's iOS Developer Library, which made the following statements.

i) "Get information from iOS, when appropriate. People store lots of information on their devices. When it makes sense***, don't force people to give you information you can easily find for yourself, such as their contacts*** or calendar information."

ii) "It's often said that ***people spend no more than a minute or two evaluating a new app. ... Avoid displaying an About window or a splash screen***. In general, try to ***avoid providing any type of startup experience that prevents people from using your application immediately. Delay a login requirement for long as possible***. Ideally, users should be able to navigate through much of your app and understand what they can do with it before logging in."

iii) "If possible, ***avoid requiring users to indicate their agreement to your EULA when they first start your application.*** Without an agreement displayed, users can enjoy your application without delay."

89. Thus, in direct conflict with the customer assurances and standards it espoused and purportedly mandated, Apple's *iOS Human Interface Guidelines* manual taught and suggested App developers to design and build Apps that: (a) directly and automatically accessed address books—particularly whenever the developer may desire it for collaborative or sharing purposes—without any prior alert(s) to the App user; and (b) download, operate, and function in

advance of any presentation of or user consent to an End User License Agreement ("EULA") or privacy policy. In accord with Apple's instructions, the App Defendants to Plaintiffs' recollection did not present either an EULA, terms of service, privacy policies or any other terms to Plaintiffs in advance of the download, installation, activation and initial operation on Plaintiffs' respective iDevices of each App Defendants' respective App.

Actions of the Specific App Defendants Sued Here

90. Each of the App Defendants here created and distributed an App, in conjunction with Apple, which improperly invaded Plaintiffs' privacy and misappropriated address book data stored in the iDevices' Contacts App without authorization to do so. Each App Defendant and Apple also worked together to jointly develop each App in question, to knowingly, collaboratively and repeatedly deploy on Plaintiffs' and Class Members' iDevices the Apps in question, which improperly invaded Plaintiffs' privacy and misappropriated address book data as stored in the iDevices' Contacts App without authorization to do so.

91. The App Defendants each followed Apple's standard protocol for placing the Apps in question for distribution in the App Store. Each App Defendant collaborated with Apple to place their App for distribution in the App Store, collaborated with Apple to distribute the App through the App Store, and actually deployed their Apps to consumers in collaboration with Apple through the App Store.

92. Plaintiffs were not made aware of, nor did they consent to the taking of their data by the App Defendants.

Gowalla

93. App Defendant Gowalla built the Gowalla App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Gowalla App on the App Store and served as Gowalla's agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

94. Without prior user consent, the Gowalla App uploaded iDevice address book data to Gowalla or someone acting on its behalf. As a consequence, Gowalla improperly obtained the address book data belonging to Plaintiffs and class members.

95. Apple did not remove the Gowalla App from the App Store even after being advised of its data theft. The Gowalla App remained available on the App Store to iDevice owners for more than a year after that, until it shut down.

96. Plaintiffs Beurhasen, Dean, King, Mandaywalla, Paul, Sandiford and Varner (the "Gowalla Plaintiffs") each recall using the Gowalla App, logging in and navigating within the App to a "Find Friends" menu screen, and being offered various options (including an option entitled "Address Book").

97. Gowalla benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Hipster

98. Hipster has already been served with process twice in the above-captioned lead case through its registered Delaware agent for service of process, Agents and Corporations, Inc., 1201 Orange Street, Suite 600, One Commerce Center, Delaware 19801, but has not appeared and default has been entered against it on the Plaintiffs' Second Amended Complaint. Dkt. Nos. 103, 346. Solely as against Hipster and in furtherance of that entry of default and to pursue default judgment, Plaintiffs (Plaintiff King particularly) from the lead *Opperman* case maintain the allegations and claims of their Second Amended Complaint, Dkt. No. 103, against Hipster. Accordingly, the current pleading is not meant to amend the prior complaint as to Hipster.

Kik Interactive

99. App Defendant Kik Interactive built the Kik Messenger App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Kik

Messenger App on the App Store and served as Kik Interactive's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

100. Without prior user consent, the Kik Messenger App uploaded iDevice address book data to Kik Interactive or someone acting on its behalf. As a consequence, Kik Interactive improperly obtained the address book data belonging to Plaintiffs and class members.

101. Apple knew this was transpiring. Kik Messenger's viral growth taxed Apple servers. Plus, reporters wrote up numerous reports with titles like, "Speedy Messenging App Kik Goes Viral, But is It Cool With Apple's T[erms]O[f]S[ervice]?" and contacted Apple for answers to these questions. Apple chose not to comment or warn consumers. Apple did not remove the App from the App Store.

102. Plaintiffs Dennis-Cooley and Green (the "Kik Interactive Plaintiffs") each recall using the Kik Messenger App, logging in, and navigating within the App.

103. Kik Interactive benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Path

104. App Defendant Path built the Path App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Path App on the App Store and served as Path's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

105. Without prior user consent, the Path App uploaded iDevice address book data to Path or someone acting on its behalf. As a consequence, Path improperly obtained the address book data belonging to Plaintiffs and class members.

106. Apple is a joint-venturer in the iFund venture capital fund and mentoring program ("iFund"). Path is an iFund company. On information and belief, Apple owns a portion of the

iFund and provided mentoring to iFund-financed companies (including Path) and the iFund owns or owned a portion of Path's equity. On information and belief, Apple provided direct guidance, assistance, and mentoring to Path on its Path App and knew that Path was uploading consumers' address books.

107. On or about February 8, 2013, Path entered into a Consent Decree with the United States Department of Justice enjoining it from, *inter alia*, continuing to misrepresent to consumers the extent to which it maintains and protects the privacy and confidentiality of information stored on iDevices, including users' address books.

108. Plaintiffs Carter, Dennis-Cooley, Green, and Paul (the "Path Plaintiffs"), each recalls opening the Path App, signing up via a "Sign Up" screen, and using and navigating around the App.

109. Path benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Foursquare Labs

110. App Defendant Foursquare Labs built the Foursquare App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Foursquare App on the App Store and served as Foursquare Labs' world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

111. Without prior user consent, the Foursquare App uploaded iDevice address book data to Foursquare Labs or someone acting on its behalf. As a consequence, Foursquare Labs improperly obtained the address book data belonging to Plaintiffs and class members.

112. Plaintiffs Beuershausen, Hoffman, King, Mandaywala, Paul, Sandiford and Varner (the "Foursquare Labs Plaintiffs") obtained the Foursquare App and recall signing up and

logging in on the Foursquare App's sign-up/log-in screen prior to February 2012 and then using and navigating around the App.

113. Foursquare Labs benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Instagram

114. App Defendant Instagram built the Instagram App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Instagram App on the App Store and served as Instagram's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

115. Without prior user consent, the Instagram App uploaded iDevice address book data to Instagram or someone acting on its behalf. As a consequence, Instagram improperly obtained the address book data belonging to Plaintiffs and class members.

116. Plaintiffs Biondi, Dennis-Cooley, Green, Hoffman, King, Mandaywala, Moses, Sandiford, and Varner (the "Instagram Plaintiffs") recall using and navigating around the Instagram App.

117. Instagram benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Yelp

118. App Defendant Yelp built the Yelp! App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Yelp! App on the App Store and

served as Yelp's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

119. Without prior user consent, the Yelp! App uploaded iDevice address book data to Yelp or someone acting on its behalf. As a consequence, Yelp improperly obtained the address book data belonging to Plaintiffs and class members.

120. Plaintiffs Biondi, Hodgins, Hoffman, Mandaywala, and Paul (the "Yelp Plaintiffs") each recall navigating to various screens on and using the Yelp! App. They recall providing a log in and navigating within the Yelp! App to a screen containing a ["Find Friends"] button with the accompanying displayed text: "Find friends on Yelp using your Contacts and Facebook friends? You'll be able to see their bookmarks and find out when they're nearby. [Yes, Find Friends] [No, Skip This]", and pressing the ["Yes, Find Friends"] button. Plaintiffs do not recall being presented at any time in that process with an intervening alert or pop-up display indicating that the Yelp! App would transfer any portion of his or her private address book to Yelp to perform this function or warning that such a transmission was about to occur.

121. Yelp benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Twitter

122. App Defendant Twitter built the Twitter App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Twitter App on the App Store and served as Twitter's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

123. Without prior user consent, the Twitter App uploaded iDevice address book data to Twitter or someone acting on its behalf. As a consequence, Twitter improperly obtained the address book data belonging to Plaintiffs and class members.

124. Plaintiffs Beuershausen, Biondi, Dean, Dennis-Cooley, Green, Hodgins, Hoffman, King, Mandaywala, Moses, Paul, Sandiford, and Varner (the "Twitter Plaintiffs") recall opening the Twitter App, signing up via its displayed registration screen, and using the App. They were initially presented a "Welcome" screen prompting them to press an on-screen button labeled ["Follow your friends"], under which was written in small type: "Scan your contacts for people you already know on Twitter." They also recall another screen labeled "Follow Friends" that similarly prompted them to press an on-screen button labeled ["Follow your friends"], under which was written in small type the identical phrase as before.

125. Twitter benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Foodspotting

126. App Defendant Foodspotting built the Foodspotting App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Foodspotting App on the App Store and served as Foodspotting's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

127. Without prior user consent, the Foodspotting App uploaded iDevice address book data to Foodspotting or someone acting on its behalf. As a consequence, Foodspotting improperly obtained the address book data belonging to Plaintiffs and class members.

128. Plaintiffs King and Sandiford (the "Foodspotting Plaintiffs") recall opening the Foodspotting App, signing up via its registration screen, and using the App. More particularly, they recall navigating to the Foodspotting App's "Follow People" screen containing an on-screen button labeled ["Find iPhone Contacts."]. While on that screen, the Foodspotting Plaintiffs tapped that button. The screen contained no warnings whatsoever indicating that the App was relaying his or her address book to Foodspotting.

129. Foodspotting benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Rovio & Chillingo

130. On information and belief, App Defendant Rovio built the Angry Birds Classic, with Defendant Chillingo providing its Crystal Platform as integrated into the App, using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Angry Birds Classic App on the App Store and served as Rovio and Chillingo's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

131. Without prior user consent, the Angry Birds Classic App uploaded iDevice address book data to Rovio and/or Chillingo or someone acting on its behalf. As a consequence, Rovio and/or Chillingo improperly obtained the address book data belonging to Plaintiffs and class members.

132. Plaintiffs Beuershausen, Dean, Green, Hodgins, Mandaywala, Sandiford and Varner (the "The Rovio and Chillingo Plaintiffs") recall opening the Angry Birds Classic App, playing Angry Birds, and navigating around to other screens and menus within the App. On information and belief, Plaintiffs' address book data was uploaded without their consent during their use of Angry Birds Classic App.

133. Rovio and Chillingo benefitted substantially from their misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the companies to more rapidly grow their user bases, avoid the costs of customer acquisition, enhance their social networking features, and increase the value of the companies, among other benefits.

ZeptoLab, Chillingo & Electronic Arts

134. On information and belief, App Defendant ZeptoLab built the Cut the Rope App, with Defendant Chillingo providing its Crystal Platform as integrated into the App by using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Cut the Rope App on the App Store and served as ZeptoLab and Chillingo's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

135. Without prior user consent, the Cut the Rope App uploaded iDevice address book data to ZeptoLab and/or Chillingo or someone acting on its behalf. As a consequence, ZeptoLab and/or Chillingo improperly obtained the address book data belonging to Plaintiffs and class members.

136. Plaintiffs Biondi, Green, Hodgins, Mandaywala, Sandiford and Varner (the "ZeptoLab and Chillingo Plaintiffs") recall opening the Cut the Rope App, playing some games of Cut the Rope, and navigating around to other screens and menus within the App. On information and belief, Plaintiffs' address book data was uploaded without their consent during their use of the Cut the Rope App.

137. ZeptoLab and Chillingo benefitted substantially from their misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the companies to more rapidly grow their user bases, avoid the costs of customer acquisition, enhance their social networking features, and increase the value of the companies, among other benefits.

138. Defendant Electronic Arts acquired Chillingo around October 2010 and has operated Chillingo as a reporting division or wholly-owned, joint-reporting subsidiary of Electronic Arts. On information and belief, Electronic Arts has controlled Chillingo since October 2010 and directed and is aware of its business operations, including with respect to Crystal and the Gaming Program. On information and belief, Electronic Arts is a successor-in-interest to or is vicariously liable for Chillingo's obligations and liabilities, including its joint and

several liabilities alleged herein pertaining to the Cut the Rope App, the Angry Birds Classic App, and the Crystal platform.

Each Plaintiff Was Injured by The Defendants

Allen Beuershausen

139. To the best of Plaintiff Allen Beuershausen's recollection, he purchased an iPhone 3G in approximately mid-2009. He subsequently purchased an iPhone 3S in mid-2011, an iPhone 4S in mid-2013, and another iPhone 4S as a replacement. He has consistently owned and used an iPhone since 2009.

140. Beuershausen downloaded the following Apps made by the App Defendants: Angry Birds Classic, Foursquare, Gowalla, and Twitter. Each of those Apps took Beuershausen's address book data without his consent.

141. Beuershausen purchased his iPhone with the expectation that address book data stored on his iDevice would be secure, and could not be accessed or copied by third parties, including through Apps, without his express consent.

142. If Beuershausen had known that his address book data stored on his iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent, then he would not have paid as much for the iDevice.

143. At no time did Apple disclose to Beuershausen that his address book data stored on his iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent.

144. Beuershausen viewed and relied on information disseminated by Apple concerning the security features of iDevices. Specifically, he was exposed to Apple's publicity campaign as follows:

i) Beuershasen viewed Apple television advertisements as well as statements and news reports regarding Apple products and Apple representations, including those emphasizing the resistance of Apple iOS-based products to malware and viruses. Beuershasen generally reads or watches both traditional and non-traditional media, and is exposed to marketing and

publicity material in a variety of forms. Through that exposure, Beuershasen has viewed numerous advertisements and reports about Apple's safety and security, which led to his confidence in those features of Apple's products.

ii) Beuershasen was exposed to the above statements by Apple and received invoice email communication from Apple touting its respect for his privacy prior to purchasing one or more iDevices.

iii) Beuershasen conducted research regarding the iDevice product and its features, including security, through operation of earlier iterations of iDevices and being exposed to its features.

iv) Beuershasen relied on the Apple statements he viewed through both traditional and non-traditional media when he decided to purchase an iDevice.

Giuliana Biondi

145. To the best of Plaintiff Giuliana Biondi's recollection, she purchased an iPhone 3G in early 2009. Biondi subsequently purchased an iPhone 4 in early 2010, and iPhone 4S in April 2012. She has consistently owned and used an iPhone since 2009

146. Biondi downloaded the following Apps made by the App Defendants: Cut the Rope, Instagram, Twitter, and Yelp!. Each of those Apps took Biondi's address book data without her consent.

147. Biondi purchased her iPhone with the expectation that address book data stored on her iDevice would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

148. If Biondi had known that her address book data stored on her iPhone was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iPhone.

149. At no time did Apple disclose to Biondi that her address book data stored on her iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent.

150. Biondi viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, she was exposed to Apple's publicity campaign as follows:

i) Biondi generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Biondi has viewed numerous advertisements and reports about Apple's safety and security, which led to her confidence in those features of Apple's products.

ii) Biondi was exposed to the above statements by Apple prior to purchasing an iPhone.

iii) Biondi recalls representations to the effect that Apple's phones and mobile products were safe, including the Apple ID and password feature of the App Store and iDevices, as well as a television advertisement that depicted Apple computers as virus-free.

iv) Biondi relied on Apple's representations regarding safety when she decided to purchase an iPhone.

Lauren Carter

151. To the best of Plaintiff Lauren Carter's recollection, she purchased an iPhone in December 2011. She has consistently had an iPhone since December 2011.

152. Carter downloaded the Path App. This App took Carter's address book data without her consent.

153. Carter purchased her iPhone with the expectation that address book data stored on her iDevice would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

154. If Carter had known that her address book data stored on her iPhone was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iPhone.

155. At no time did Apple disclose to Carter that her address book data stored on her iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent.

156. Carter viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, she was exposed to Apple's publicity campaign as follows:

i) Carter generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Carter has viewed numerous advertisements and reports about Apple's safety and security, which led to her confidence in those features of Apple's products.

ii) Carter was exposed to the above statements by Apple prior to purchasing an iPhone.

iii) Carter recalls representations to the effect that Apple's phones and mobile products were safe, including the Apple ID and password feature of the App Store.

iv) Carter relied on Apple's representations regarding safety when she decided to purchase an iPhone.

Stephanie Dennis-Cooley

157. To the best of Plaintiff Stephanie Dennis-Cooley's recollection, she purchased an iPhone 3G on or around July 2008. She has subsequently purchased an iPhone 4 in 2010 and an iPhone 5 shortly after it was released in September 2012. She has consistently owned an iPhone since 2008.

158. Dennis-Cooley also purchased a first-generation iPad a few months after it was released on or around April 3, 2010. She subsequently purchased another iPad in 2011. She has consistently owned an iPad since mid-2010.

159. Dennis-Cooley downloaded the following Apps made by the App Defendants: Instagram, Kik Messenger, Path, and Twitter. Each of those Apps took Dennis-Cooley's address book data without her consent.

160. Dennis-Cooley purchased her iDevices with the expectation that address book data stored on her iDevices would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

161. If Dennis-Cooley had known that her address book data stored on her iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iDevices.

162. At no time did Apple disclose to Dennis-Cooley that her address book data stored on her iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent.

163. Dennis-Cooley viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, she was exposed to Apple's publicity campaign as follows:

i) Dennis-Cooley viewed Apple television advertisements and presentations by Stephen Jobs. She generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Dennis-Cooley has viewed numerous advertisements and reports about Apple's safety and security, which led to her confidence in those features of Apple's products.

ii) Dennis-Cooley was exposed to the above statements by Apple prior to purchasing an iPhone.

iii) Dennis-Cooley recalls the television advertisement about Apple's computers being safe from computer viruses.

iv) Dennis-Cooley relied on representations that Apple products were safe when she decided to purchase an iDevice.

Stephen Dean

164. To the best of Plaintiff Stephen Dean's recollection, he purchased a first-generation iPhone in late 2007. He subsequently purchased an iPhone 3G in approximately October 2008, and an iPhone 4 in July 2010, and an iPhone 5 in February 2013. Dean has consistently owned and used the iPhone since 2007.

165. Dean also purchased an iPad in 2009. He subsequently purchased an iPad mini in summer 2013. He has consistently owned and used an iPad since 2009.

166. Dean downloaded the following Apps made by the App Defendants: Angry Birds Classic, Gowalla, and Twitter. Each of those Apps took Dean's address book data without his consent.

167. Dean purchased his iDevices with the expectation that address book data stored on his iDevices would be secure, and could not be accessed or copied by third parties, including through Apps, without his express consent.

168. If Dean had known that his address book data stored on his iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent, then he would not have paid as much for the iDevices.

169. At no time did Apple disclose to Dean that his address book data stored on his iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent.

170. Dean viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, he was exposed to Apple's publicity campaign as follows:

i) Dean viewed television advertisements, Apple advertising and marketing statements, as well as articles regarding the statements, online research of Apple productions from third-party websites as well as Apple's website and product descriptions. Dean generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Dean has viewed numerous advertisements and reports about Apple's safety and security, which led to his confidence in those features of Apple's products.

ii) Dean was exposed to the above statements by Apple prior to purchasing an iDevice.

iii) Dean recalls the television advertisement about Apple's computers being safe from computer viruses, he generally recalls statements that Apple's products were safe and secure.

iv) ean relied on these statements and representations when he decided to purchase an iDevice.

Jason Green

171. To the best of Plaintiff Jason Green's recollection, he purchased an iPhone 3G in approximately September 2008. He subsequently purchased an iPhone 4 in or around September 2010. He has consistently had an iPhone since 2008.

172. Green downloaded the following Apps made by the App Defendants: Angry Birds Classic, Cut the Rope, Instagram, Kik Messenger, Path, and Twitter. Each of those Apps took Green's address book data without his consent.

173. Green purchased his iPhone with the expectation that address book data stored on his iDevice would be secure, and could not be accessed or copied by third parties, including through Apps, without his express consent.

174. If Green had known that his address book data stored on his iPhone was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent, then he would not have paid as much for the iPhone.

175. At no time did Apple disclose to Green that his address book data stored on his iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent.

176. Green viewed and relied on information disseminated by Apple concerning the security of iDevices. Green generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Green has viewed numerous advertisements and reports about Apple's safety and security, which led to his confidence in those features of Apple's products.

Claire Hodgins

177. To the best of Plaintiff Claire Hodgins's recollection, she purchased an iPhone 4 in 2011. She has subsequently purchased an iPhone 4S in 2012. She has consistently owned and used an iPhone since 2008.

178. Hodgins downloaded the following Apps made by the App Defendants: Angry Birds Classic, Cut the Rope, Twitter, and Yelp!. Each of those Apps took Hodgins's address book data without her consent.

179. Hodgins purchased her iPhone with the expectation that address book data stored on her iDevice would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

180. If Hodgins had known that her address book data stored on her iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iDevice.

181. At no time did Apple disclose to Hodgins that her address book data stored on her iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent.

182. Hodgins viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, she was exposed to Apple's publicity campaign as follows:

i) Hodgins generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Hodgins has viewed numerous advertisements and reports about Apple's safety and security, which led to her confidence in those features of Apple's products.

ii) Hodgins was exposed to the above statements by Apple prior to purchasing an iPhone.

iii) Hodgins relied on the Apple statements she viewed through both traditional and non-traditional media when she decided to purchase an iPhone.

Gentry Hoffman

183. To the best of Plaintiff Gentry Hoffman's recollection, he purchased an iPhone 3 approximately two weeks after it was released on or around July 11, 2008. Hoffman subsequently purchased an iPhone 3G around July 2008; an iPhone 4 around October 2011; an iPhone 4S around September 2012; and an iPhone 5 around September 2013. Hoffman has consistently owned and used an iPhone since 2008.

184. Hoffman downloaded the following Apps made by the App Defendants: Foursquare, Instagram, Twitter, and Yelp! prior to February 2012. Each of those Apps took Hoffman's address book data without his consent.

185. Hoffman purchased his iPhone with the expectation that address book data stored on his iDevice would be secure, and could not be accessed or copied by third parties, including through Apps, without his express consent.

186. If Hoffman had known that his address book data stored on his iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent, then he would not have paid as much for the iDevice.

187. At no time did Apple disclose to Hoffman that his address book data stored on his iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent. Hoffman viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, he was exposed to Apple's publicity campaign as follows:

i) Hoffman viewed statements made by Apple and its representatives at Apple conferences, presentations, product release events and in other technology media sources and interviews. He watched several of Apple's yearly product launch events, and would often observe a live blog of such events. Hoffman generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Hoffman has viewed numerous

advertisements and reports about Apple's safety and security, which led to his confidence in those features of Apple's products.

ii) Hoffman was exposed to the above statements by Apple as early as 2007, but in any event prior to purchasing an iPhone.

iii) Hoffman recalls numerous representations to the effect that Apple's phones and mobile products were more secure generally, in particular, that they better protected against theft of personal information, and that they actively protected users' private information.

iv) Hoffman relied on Apple's representations regarding privacy, personal information security, a more secure App ecosystem, and tougher vetting process for Apps to keep his information safe. In particular, Apple's representations that its products would keep his information safer than other companies' products was a significant factor in his decision to purchase an iDevice.

Rachelle King

188. To the best of Plaintiff Rachelle King's recollection, she pre-ordered and purchased the first generation iPhone in 2007. King subsequently purchased an iPhone 3G in 2008. King has consistently owned and used an iPhone since 2007.

189. King also purchased an iPad in March 2010.

190. King downloaded the following Apps made by the App Defendants: Foodspotting, Foursquare, Gowalla, Hipster, Instagram, and Twitter prior to February 2012. Each of those Apps took King's address book data without her consent.

191. King purchased her iDevices with the expectation that address book data stored on her iDevices would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

192. If King had known that her address book data stored on her iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iDevices.

193. At no time did Apple disclose to King that her address book data stored on her iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent. King viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, she was exposed to Apple's publicity campaign as follows:

i) King viewed statements made by Apple and its representatives at Apple conferences, presentations, product release events and in other technology media sources and interviews. She watched several of Apple's yearly product launch events. King generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, King has viewed numerous advertisements and reports about Apple's safety and security, which led to her confidence in those features of Apple's products.

ii) King was exposed to the above statements by Apple as early as 2007, but in any event prior to purchasing an iDevice.

iii) King recalls representations to the effect that Apple's products were more secure generally than other similar devices.

iv) King relied on Apple's representations as a factor in her decision to purchase an iDevice.

Nirali Mandalaywala

194. To the best of Plaintiff Nirali Mandalaywala's recollection, she purchased a first generation iPhone in or around January 2008. She has subsequently purchased an iPhone 3G, 4, 4S, and most recently an iPhone 5S in November 2013. She has consistently owned and used an iPhone since January 2008.

195. Mandalaywala downloaded the following Apps made by the App Defendants: Angry Birds Classic, Cut the Rope, Foursquare, Gowalla, Instagram, Twitter, and Yelp!. Each of those Apps took Mandalaywala's address book data without her consent.

196. Mandalaywala purchased her iPhone with the expectation that address book data stored on her iDevice would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

197. If Mandalaywala had known that her address book data stored on her iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iDevice.

198. At no time did Apple disclose to Mandalaywala that her address book data stored on his iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent.

199. Mandalaywala viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, she was exposed to Apple's publicity campaign as follows:

i) Mandalaywa viewed statements made by Apple and its representatives at Apple conferences, presentations, keynote speeches, product release events, and in other technology media blogs, as well as television advertisements. Mandalaywala generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Mandalaywala has viewed numerous advertisements and reports about Apple's safety and security, which led to her confidence in those features of Apple's products.

ii) Mandalaywala was exposed to the above statements by Apple prior to purchasing an iPhone.

iii) Mandalaywala recalls numerous representations that Apple's products were safe and secure, such as the television advertisement about Apple's computers being safe from computer viruses.

iv) Mandalaywala relied on Apple's representations regarding the safety and security of Apple's iDevices when she decided to purchased an iPhone.

Claire Moses

200. To the best of Plaintiff Claire Moses's recollection, she received an iPhone 3G in December 2008. She has subsequently received an iPhone 4S in January 2012. She has consistently owned and used an iPhone since 2008.

201. Moses downloaded the following Apps made by the App Defendants: Instagram and Twitter. Each of those Apps took Moses's address book data without her consent.

202. Moses purchased her iPhone with the expectation that address book data stored on her iDevice would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

203. If Moses had known that her address book data stored on her iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iDevice.

204. At no time did Apple disclose to Moses that her address book data stored on her iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent.

205. Moses viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, she was exposed to Apple's publicity campaign as follows:

iv) Moses generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Moses has viewed numerous advertisements and reports about Apple's safety and security, which led to her confidence in those features of Apple's products.

v) Moses was exposed to the above statements by Apple prior to purchasing an iPhone.

vi) Moses relied on the Apple statements she viewed through both traditional and non-traditional media when she decided to purchase an iPhone.

Judy Paul

206. To the best of Plaintiff Judy Paul's recollection, she purchased a first-generation iPhone in August 2008. She subsequently purchased an iPhone 4 in September 2010, and 5S in February 2014. She has consistently used an iPhone since 2008.

207. Paul also purchased an iPad in December 2011.

208. Paul downloaded the following Apps made by the App Defendants: Foursquare, Gowalla, Path, Twitter, and Yelp!. Each of those Apps took Paul's address book data without her consent.

209. Paul purchased her iDevices with the expectation that address book data stored on her iDevices would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

210. If Paul had known that her address book data stored on her iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iDevices.

211. At no time did Apple disclose to Paul that her address book data stored on her iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent.

212. Paul viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, she was exposed to Apple's publicity campaign as follows:

i) Paul viewed television advertisements, product launch statements and press releases by Apple and its representatives. She generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Paul has viewed numerous advertisements and reports about Apple's safety and security, which led to her confidence in those features of Apple's products.

ii) Paul was exposed to the above statements by Apple prior to purchasing an iDevice.

iii) Paul recalls the television advertisement about Apple's computers being safe from computer viruses.

iv) Paul relied on representations that Apple products were safe when she decided to purchase an iDevice. Specifically, she trusted Apple in the same way that she trusts her bank with her private information.

Maria Pirozzi

213. To the best of Plaintiff Maria Pirozzi's recollection, she purchased her iPhone 4 in or about September 2011.

214. Following her purchase of her iPhone, she downloaded a number of apps from the App Store, including the Facebook and Angry Birds apps.

215. Pirozzi purchased her iPhone with the expectation that address book data stored on her iDevice would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

216. If Pirozzi had known that her address book data stored on her iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iDevice.

217. At no time did Apple disclose to Pirozzi that her address book data stored on her iDevice was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent.

218. Before purchasing her iPhone in September 2011, Pirozzi visited Apple's website as well as viewed Apple's in-store advertisements. In addition, Pirozzi relied on Apple's reputation for safety and security.

Theda Sandiford

219. To the best of Plaintiff Theda Sandiford's recollection, she purchased an iPad in summer 2010. She subsequently purchased on iPad 2 in March 2012. Sandiford has consistently had an iPad since 2010.

220. Sandiford also purchased an iPhone in 2012.

221. Sandiford downloaded the following Apps made by the App Defendants: Angry Birds Classic, Cut the Rope, Foodspotting, Foursquare, Gowalla, Instagram, and Twitter. Each of those Apps took Sandiford's address book data without her consent.

222. Sandiford purchased her iDevices with the expectation that address book data stored on her iDevices would be secure, and could not be accessed or copied by third parties, including through Apps, without her express consent.

223. If Sandiford had known that her address book data stored on her iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without her express consent, then she would not have paid as much for the iDevices.

224. At no time did Apple disclose to Sandiford that her address book data stored on her iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent.

225. Sandiford viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, she was exposed to Apple's publicity campaign as follows:

i) Sandiford generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Pirozzi has viewed numerous advertisements and reports about Apple's safety and security, which led to her confidence in those features of Apple's products.

ii) Sandiford was exposed to the above statements by Apple prior to purchasing an iPhone.

iii) Sandiford relied on the Apple statements she viewed through both traditional and non-traditional media when she decided to purchase an iDevice.

Gregory Varner

226. To the best of Plaintiff Gregory Varner's recollection, he purchased an iPhone in September 2007. He has subsequently purchased an iPhone 3 in 2008, an iPhone 3G in mid-

2009, an iPhone 4 in late 2011, and an iPhone 5 on or around late 2013. Varner has consistently owned and used an iPhone since 2007.

227. Varner also purchased a first-generation iPad within approximately 45 days of its release on or around April 3, 2010. He subsequently purchased an iPad 3 within approximately 45 days of its release on or around March 16, 2012. He has consistently owned and used an iPad since 2010.

228. Varner downloaded the following Apps made by the App Defendants: Angry Birds Classic, Cut the Rope, Foursquare, Gowalla, Instagram, and Twitter prior to February 2012. Each of those Apps took Varner's address book data without his consent.

229. Varner purchased his iDevices with the expectation that address book data stored on his iDevices would be secure, and could not be accessed or copied by third parties, including through Apps, without his express consent.

230. If Varner had known that his address book data stored on his iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent, then he would not have paid as much for the iDevices.

231. At no time did Apple disclose to Varner that his address book data stored on his iDevices was not secure, and could be accessed or copied by third parties, including through Apps, without his express consent.

232. Varner viewed and relied on information disseminated by Apple concerning the security of iDevices. Specifically, he was exposed to Apple's publicity campaign as follows:

i) Varner viewed Apple statements on videos and online, reading Gizmodo, Engadget, and MacLife blogs that covered Apple product launches, viewing Mr. Jobs' interviews and presentations regarding Apple's iDevices. Varner generally reads or watches both traditional and non-traditional media, and is exposed to marketing and publicity material in a variety of forms. Through that exposure, Varner has viewed numerous advertisements and reports about Apple's safety and security, which led to his confidence in those features of Apple's products.

ii) Varner was exposed to the above statements by Apple prior to purchasing an iPhone.

iii) Varner recalls representations that Apple emphasized security of its iDevices and products. He further recalls representations that Apple's App Store was secure because it was created by Apple.

Varner relied on Apple's representations regarding security and trusted Apple with his private information, including his address book, when he decided to purchase an iDevice.

CLASS ACTION ALLEGATIONS

233. Plaintiffs bring this lawsuit as a class action under Rules 23(a), 23(b)(1), 23(b)(2) and/or 23(b)(3) of the Federal Rules of Civil Procedure on behalf of a class of similarly situated persons consisting of:

The iDevice Class: All United States residents who purchased iDevices between July 10, 2008 and February 2012.

The Address Book Misappropriation Subclasses: All members of the iDevice Class on whose iDevice one or more of the following Apps was installed: Angry Birds Classic (with integrated Crystal platform), Cut the Rope (with integrated Crystal platform), Foursquare, Foodspotting, Gowalla, Hipster, Kik Messenger, Instagram, Path, Twitter, or Yelp! iDevice Apps.

234. **Numerosity.** The members of the Class, who are ascertainable from Defendants' records, are so numerous that joinder of all members is impracticable. The Class is likely to exceed five million members from reported iDevice sales figures and reported user- bases for the identified Apps.

235. **Typicality.** Plaintiffs' claims are typical of the claims of the members of the Class. Plaintiffs and all members of the Class purchased an Apple iDevice, maintained his or her private address book with that iDevice, installed one or more identified iDevice Apps from Apple, and have sustained damages arising out of Defendants' conduct.

236. **Commonality.** Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members. Questions of law and fact common to the Class include:

i) Whether Defendant Apple advertised the iDevices as safe and secure;

ii) Whether Defendant Apple knew and failed to disclose that the iDevices' Contacts App and the address books contained therein were not safe and secure from third-party Apps;

iii) What security features were included in Apple's iDevices for safeguarding the Contacts App's address books;

iv) Whether Defendant Apple provided App Defendants with guidelines or other resources to develop Apps with the ability to access and copy users' address book data;

v) Whether each App Defendants uploaded Plaintiffs' address books from Plaintiffs' iDevices;

vi) What benefits each App Defendant gained as a result of its misappropriation of class members' address books;

vii) What representations were made by Apple concerning the security of its iDevices;

viii) What material information Apple knew but failed to disclose concerning the security of its iDevices, and its legal obligation to disclose such information;

ix) Whether iDevice owners have a privacy and property interest in their address book data;

x) Whether acquisition of users' address book data without their consent violates their right to privacy;

xi) The proper measure and amount of damages or other recovery available to the class; and

xii) The unjust enrichment realized by any Defendants.

237. **Adequacy.** Plaintiffs will continue to fairly and adequately represent the interests of the class and have no interests adverse to or in conflict with other class members. Plaintiffs' retained counsel have and will continue to vigorously prosecute this case, have previously been designated class counsel on cases in this judicial district, and are highly experienced in class and complex, multi-party litigation matters.

238. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because, among other things, joinder of all class members is impracticable and a class action will reduce the risk of inconsistent adjudications or repeated litigation on the same conduct. Further, the expense and burden of individual lawsuits would make it virtually impossible for class members, Defendants, or the Court to cost-effectively redress separately the unlawful conduct alleged. Thus, absent a class action, Defendants would unjustly retain the benefits of their wrongdoings. Plaintiffs know of no difficulties to be encountered in the management of this action that would preclude its maintenance as a class action, either with or without sub-classes.

239. The State of California has sufficient state interest through a significant contact or aggregation of contacts to the claims asserted by each member of the Class so that the choice of California law is not arbitrary or unfair.

240. Adequate notice can be given to Class members directly using information maintained in Apple's and other Defendants' records, or through notice by publication.

241. Accordingly, class certification is appropriate under Rule 23.

CLAIMS FOR RELIEF

242. Based on the foregoing allegations, Plaintiffs make the following claims for relief. As indicated at each cause of action below, each claim is asserted by various Plaintiffs on behalf of themselves and the applicable Class. Except as otherwise specifically indicated, each claim incorporates all of the allegations of this Complaint as if set forth fully therein.

Count One
Invasion of Privacy (Intrusion upon Seclusion)
(*Against All Defendants on Behalf of All Plaintiffs*)

243. Each Plaintiff, on his or her own behalf and on behalf of all class members,

incorporates the above allegations by reference as if fully set forth herein, and further alleges as follows:

244. Plaintiffs have reasonable expectations of privacy in their iDevices and their mobile address books.

245. The Plaintiffs' private affairs include the contents of their iDevices, their private address books, and those address books' unique contacts and fields, which identify persons with whom Plaintiffs associate and communicate. These are not matters of legitimate public concern.

246. By surreptitiously obtaining, improperly gaining knowledge, reviewing and retaining Plaintiffs' private address books (or substantial portions thereof) as stored in the Contacts App on Plaintiffs' iDevices, the App Defendants intentionally intruded on and into each respective Plaintiff's solitude, seclusion or private affairs.

247. The App Defendants intrusions were highly offensive to a reasonable person. These intrusions were so highly offensive that myriad newspaper articles, blogs, op-eds, and investigative exposés were written complaining and objecting vehemently to these defendants' practices, Congressional inquiries were opened to investigate these practices and some defendants even publicly apologized. The surreptitious manner in which the App Defendants' conducted these intrusions confirms their outrageous nature.

248. As a direct and proximate result of the respective App Defendants' actions, Plaintiffs suffered harm and damages.

249. Apple received substantial financial, economic, and advertising, public relations and other benefits from its approval, release, sale and deployment of the identified Apps.

250. Despite its ostensible policies against the collection of iDevice users' private information and public representations that Apple prohibited such misconduct, Apple in fact materially supported, assisted and helped build, market and deploy the identified Apps, and knowingly and/or recklessly permitted the unauthorized access and collection of Plaintiffs' and class members' private address books.

251. Prior to February 2012, Apple never instructed App Defendant to design its App to include any user alerts or permission dialogue boxes to ensure user consent before the

collection of address books, and even thereafter failed to take steps to ensure that alerts and dialogue boxes were sufficient to provide actual notice and sufficient consent. Apple's encouragement, assistance and support were substantial factors leading to each App Defendant inflicting the above-described injuries and harms on Plaintiffs and class members and a proximate cause of their damages.

252. In so doing, Apple aided and abetted the foregoing misconduct of the App Defendants and is liable for the resulting harm to Plaintiffs and class members.

253. Defendants' conduct described herein was willful, malicious and oppressive, and constitutes despicable conduct in conscious disregard of the rights of Plaintiffs and the class.

254. As a result of Defendants' conduct described herein, Defendants were unjustly enriched.

255. Wherefore, Plaintiffs pray for relief and judgment as set forth below.

Count Two
Conversion
(*Against All Defendants on Behalf of All Plaintiffs*)

256. Each Plaintiff, on his or her own behalf and on behalf of all class members, incorporates the above allegations by reference as if fully set forth herein, and further alleges as follows:

257. Each Plaintiff and class member owns his or her iDevice and the contents thereof, including his or her address book and all information contained therein. The information contained in each Plaintiff's and each class member's address book was compiled by or for them for their own personal use.

258. That information is the personal property of each Plaintiff and class member, and has intrinsic, extrinsic and commercial value, including to the App Defendants, who improperly made use of the information for their own benefit without consent.

259. The ownership rights of Plaintiffs and class members in their address books as stored in the Contacts App on Plaintiffs' iDevices include the exclusive right of possession and control, including exclusive right to sell, transfer, license or allow use of their address books.

260. Defendants do not have any property right in Plaintiffs' and class members'

address books and the information contained therein.

261. The App Defendants intentionally and substantially interfered with Plaintiffs' and class members' property by taking possession of the information contained in their address books, without consent.

262. That conduct deprived each Plaintiff and class member of his or her property rights in his or her mobile address book and the information contained therein, including their right to exclusive possession and control thereof.

263. The App Defendants made use of that property, benefitted from that use, and, on information and belief, profited from that use.

264. As a direct and proximate result of the foregoing, each Plaintiff and class member has been injured. That injury includes the deprivation of benefits and profits realized by the App Defendants as a result of their use of the wrongfully converted property.

265. Apple receives substantial financial, economic, and advertising, public relations and other benefits from its approval, release, sale and deployment of the identified Apps.

266. Despite its ostensible policies against the collection of iDevice users' private information and public representations that Apple prohibited such misconduct, Apple in fact materially supported, assisted and helped build, market and deploy the identified Apps, and knowingly and/or recklessly permitted the unauthorized access and collection of Plaintiffs' and class members' private mobile address book information.

267. Prior to February 2012, Apple never instructed the App Defendants to design their App to include any user alerts or permission dialogue boxes to ensure user consent before the collection of mobile address book information, and even thereafter failed to take steps to ensure that alerts and dialogue boxes were sufficient to provide actual notice and sufficient consent. Apple's encouragement, assistance and support were substantial factors leading to each App Defendant inflicting the above-described injuries and harms on Plaintiffs and class members and a proximate cause of their damages.

268. In so doing, Apple aided and abetted the foregoing misconduct of the App Defendants and is liable for the resulting harm to Plaintiffs and class members.

269. Defendants' conduct described herein was willful, malicious and oppressive, and constitutes despicable conduct in conscious disregard of the rights of Plaintiffs and the class.

270. As a result of Defendants' conduct described herein, Defendants were unjustly enriched.

271. Wherefore, Plaintiffs pray for relief and judgment as set forth below.

Count Three
Violations of False and Misleading Advertising Law (FAL)
California Business & Professions Code § 17500 *et seq.*
(Against Apple on Behalf of All Plaintiffs)

272. Each Plaintiff, on his or her own behalf and on behalf of all class members, incorporates the above allegations by reference as if fully set forth herein, and further alleges as follows:

273. Beginning on at least January 9, 2007, Apple has committed acts of untrue and misleading advertising, as defined by Business & Professions Code sections 17500 *et seq.* (the "FAL") by engaging in the following acts and practices, detailed above, with intent to induce members of the public to purchase iDevices:

i) Falsely and misleadingly representing that iDevices, and the information contained on iDevices, are safe and secure;

ii) Falsely and misleadingly representing that information contained in iDevices could not be accessed by others;

iii) Falsely and misleadingly representing that iDevice address books could not be accessed or collected by other Apps without the user's express permission;

iv) Falsely and misleadingly representing that it Apple gave users clear notice and control over the information contained in their iDevices, including address books;

v) Falsely and misleadingly representing that iDevices, including their operating system, protected users from privacy attacks;

vi) Falsely and misleadingly representing that the iDevice, and its operating

system, "sandboxed" data, including Contacts and the address books, thereby preventing other Apps from accessing that data;

vii) Falsely and misleadingly representing that Apple protected the security of personal information and other data on the iPhone;

viii) Falsely and misleadingly representing that Apple subjected Apps to an approval process that ensured that users' private data was protected, and that Apple screened iDevice Apps to prevent the dissemination of Apps that access personal information or invade users' privacy;

ix) Falsely and misleadingly representing that Apple took precautions to protect personal information on users' iDevices; and

x) Falsely and misleadingly representing that Apple fixed security issues that allowed improper access to users' private information on iDevices, including the address books.

274. Apple's statements were untrue and/or misleading. Apple knew, or by the exercise of reasonable care should have known, that they were untrue and/or misleading.

275. Apple also falsely advertised by failing to disclose the material facts set forth herein, including:

i) That iDevices, and the information contained on iDevices, were not in fact safe and secure as represented;

ii) That information contained in iDevices could in fact be accessed by others;

iii) That iDevice address books could in fact be accessed or collected by other Apps without the user's express permission;

iv) That Apple gave users clear notice and control over the information contained in their iDevices, including address books;

v) That iDevices, including their operating system, did not in fact protect users from privacy attacks;

vi) That the iDevice, and its operating system, did not in fact "sandbox" data,

including Contacts information and users' private address books, and did not prevent other Apps from accessing that data;

vii) That Apple did not in fact protect the security of personal information and other data on the iPhone;

viii) That Apple did not in fact subject Apps to an approval process that ensured that users' private data was protected, and that Apple did not in fact screen iDevice Apps to prevent the dissemination of Apps that accessed personal information or invaded users' privacy;

ix) That Apple did not in fact take the represented precautions to protect personal information on users' iDevices; and

x) That Apple did not in fact adequately fix security issues that allowed improper access to users' private information on iDevices, including address books.

276. The foregoing representations and omissions were materially misleading.

277. Apple's foregoing acts and practices did deceive and were likely to deceive Plaintiffs, class members, and the public.

278. Plaintiffs and class members relied upon the foregoing material representations and omissions to their detriment in that they would not have purchased the iDevices for the retail price paid or at all had they known of the true facts.

279. As a result of the foregoing, each Plaintiff and class member was injured in fact, and lost money or property, and each is entitled to restitution and injunctive relief.

280. As a result of the foregoing, Apple has been, and will continue to be unjustly enriched at the expense of Plaintiffs and class members.

281. Apple's foregoing misconduct is ongoing, and unless restrained by this Court, is likely to recur.

282. Defendant's conduct described herein was willful, malicious and oppressive, and constitutes despicable conduct in conscious disregard of the rights of Plaintiffs and the class.

283. Wherefore, Plaintiffs pray for relief and judgment as set forth below.

Count Four
Violations of the Consumer Legal Remedies Act (CLRA): Misrepresentation
California Civil Code, §1750 *et seq.*
(Against Apple on Behalf of All Plaintiffs)

284. Each Plaintiff, on his or her own behalf and on behalf of all class members, incorporates the above allegations by reference as if fully set forth herein, and further alleges as follows:

285. Plaintiffs are purchasers of iDevices and consumers within the meaning California Civil Code, sections 1750 *et seq.* (the "CLRA").

286. In violation of the CLRA Apple has engaged and is engaging in unfair and/or deceptive acts and practices in the course of transactions with the Plaintiffs; such transactions are intended to and have resulted in sales of merchandise. Those unfair and/or deceptive acts and practices include:

i) Representing that its goods had characteristics, uses and/or benefits which they do not have;

ii) Representing that its goods are of a particular standard, quality, and grade that they are not;

iii) Advertising its goods with intent not to sell them as advertised.

287. Specifically, Apple's past and/or ongoing conduct in violation of the CLRA include the following misrepresentations:

i) Falsely and misleadingly representing that iDevices, and the information contained on iDevices, are safe and secure;

ii) Falsely and misleadingly representing that information contained in iDevices cannot be accessed by others;

iii) Falsely and misleadingly representing that iDevice address books cannot be accessed or collected by other Apps without the user's express permission;

iv) Falsely and misleadingly representing that it Apple gives users clear notice and control over the information contained in their iDevices, including

mobile contact book data;

v) Falsely and misleadingly representing that iDevices, including their operating system, protect users from privacy attacks;

vi) Falsely and misleadingly representing that the iDevice, and its operating system, "sandbox" data, including Contacts information and users' private address books, thereby preventing other Apps from accessing that data;

vii) Falsely and misleadingly representing that Apple protects the security of personal information and other data on the iPhone;

viii) Falsely and misleadingly representing that Apple subjects Apps to an approval process that ensures that users' private data is protected, and that Apple screens iDevice Apps to prevent the dissemination of Apps that access personal information or invade users' privacy;

ix) Falsely and misleadingly representing that Apple takes precautions to protect personal information on users' iDevices; and

x) Falsely and misleadingly representing that Apple fixed security issues that allowed improper access to users' private information on iDevices, including address books.

288. The foregoing representations were/are materially misleading. At the time that Apple made the foregoing representations, Apple did not believe they were true, or had no reasonable grounds for believing they were true.

289. In addition, Apple's past and/or ongoing conduct in violation of the CLRA include its failure to disclose material facts that it was obligated to disclose because (a) Apple had exclusive knowledge of those material facts that were not known or reasonably accessible to Plaintiffs, the class, and the public; (b) Apple actively concealed those material facts from Plaintiffs, the class, and the public; and (c) the above representations by Apple, even if not deemed misrepresentations giving rise to independent liability, were partial representations that were misleading because those other material fact had not been disclosed. The material facts not disclosed by Apple in violation of the CLRA include:

i) That iDevices, and the information contained on iDevices, were not in fact safe and secure as represented;

ii) That information contained in iDevices could in fact be accessed by others;

iii) That iDevice address books could in fact be accessed or collected by other Apps without the user's express permission;

iv) That Apple gave users clear notice and control over the information contained in their iDevices, including mobile contact book data;

v) That the iDevices, including their operating system, did not in fact users from privacy attacks;

vi) That the iDevice, and its operating system, did not in fact "sandbox" data, including Contacts information and users' private address books, and did not prevent other Apps from accessing that data;

vii) That Apple did not in fact protect the security of personal information and other data on the iPhone;

viii) That Apple did not in fact subject Apps to an approval process that ensures that users' private data was protected, and that Apple did not in fact screen iDevice Apps to prevent the dissemination of Apps that access personal information or invade users' privacy;

ix) That Apple did not in fact take the represented precautions to protect personal information on users' iDevices; and

x) That Apple did not in fact adequately fix security issues that allowed improper access to users' private information on iDevices, including address books.

290. The foregoing omissions were materially misleading.

291. The foregoing omissions concerned material facts relating to deficiencies in the iDevices purchased by Plaintiffs and class members that were inherent in the products and existed at the time of purchase and at all times thereafter. Though the iDevices are covered by

a limited one-year warranty, the deficiencies at issue were present from the outset, and therefore arose and manifested within the warranty period.

292. Plaintiffs and class members relied upon the foregoing material representations and omissions to their detriment by purchasing and overpaying for iDevices that did not have the characteristics represented by Apple and which they understood the iDevices to have. Had they been aware of the facts omitted by Apple, they would not have purchased the iDevices, at least for the retail price actually paid.

293. As a result of the foregoing, each Plaintiff and class member has suffered harm.

294. Apple's violations of the CLRA have caused damage to Plaintiffs and the other Class members and threaten additional injury if the violations continue.

295. Under section 1782 of the CLRA, Apple has received notice in writing by certified mail of the particular violations of section 1770 of the CLRA from Plaintiffs on behalf of all Class members, demanding Defendant offer to resolve the problems associated with the actions detailed above and give notice to all affected consumers of the intent to so act.

296. Thirty days have passed since Plaintiffs sent their CLRA letters, by certified mail, and Apple has failed to take the actions required by the CLRA on behalf of all affected consumers. Plaintiffs and the Class are therefore entitled to all forms of relief provided under section 1780 of the CLRA.

297. Defendant's conduct described herein was willful, malicious and oppressive, and constitutes despicable conduct in conscious disregard of the rights of Plaintiffs and the class.

298. Wherefore, Plaintiffs pray for relief and judgment as set forth below.

Count Five
Deceit
Violations of the California Civil Code § 1709 *et seq.*
(Against Apple on Behalf of All Plaintiffs)

299. Each Plaintiff, on his or her own behalf and on behalf of all class members, incorporates the above allegations by reference as if fully set forth herein, and further alleges as follows:

300. By its actions described in this complaint, Defendants have committed deceit in violation of California Civil Code section 1709 *et seq*.

301. Apple's acts of deceit include making the following misrepresentations:

i) Falsely and misleadingly representing that iDevices, and the information contained on iDevices, were safe and secure;

ii) Falsely and misleadingly representing that information contained in iDevices could not be accessed by others;

iii) Falsely and misleadingly representing that iDevice address books could not be accessed or collected by other Apps without the user's express permission;

iv) Falsely and misleadingly representing that it Apple gave users clear notice and control over the information contained in their iDevices, including address books;

v) Falsely and misleadingly representing that iDevices, including their operating system, protected users from privacy attacks;

vi) Falsely and misleadingly representing that the iDevice, and its operating system, "sandboxed" data, including Contacts information and users' private address books, thereby preventing other Apps from accessing that data;

vii) Falsely and misleadingly representing that Apple protected the security of personal information and other data on the iPhone;

viii) Falsely and misleadingly representing that Apple subjected Apps to an approval process that ensureed that users' private data is protected, and that Apple screens iDevice Apps to prevent the dissemination of Apps that access personal information or invade users' privacy;

ix) Falsely and misleadingly representing that Apple took precautions to protect personal information on users' iDevices; and

x) Falsely and misleadingly representing that Apple fixed security issues that

allowed improper access to users' private information on iDevices, including address books.

302. The foregoing representations were materially misleading. At the time that Apple made the foregoing representations, Apple did not believe they were true, or had no reasonable grounds for believing they were true.

303. Apple's acts of deceit include its failure to disclose material facts that it was obligated to disclose because (a) Apple had exclusive knowledge of those material facts that were not known or reasonably accessible to Plaintiffs, the class, and the public; (b) Apple actively concealed those material facts from Plaintiffs, the class, and the public; and (c) the above representations by Apple, even if not deemed misrepresentations giving rise to independent liability, were partial representations that are misleading because those other material fact has not been disclosed. The material facts not disclosed by Apple in violation of the UCL include:

i) That iDevices, and the information contained on iDevices, were not in fact safe and secure as represented;

ii) That information contained in iDevices could in fact be accessed by others;

iii) That iDevice address books could in fact be accessed or collected by other Apps without the user's express permission;

iv) That Apple gave users clear notice and control over the information contained in their iDevices, including address books;

v) That the iDevices, including their operating system, did not in fact protect users from privacy attacks;

vi) That the iDevice, and its operating system, did not in fact "sandbox" data, including Contacts information and users' private address books, and did not prevent other Apps from accessing that data;

vii) That Apple did not in fact protect the security of personal information and other data on the iPhone;

viii) That Apple did not in fact subject Apps to an approval process that ensured that users' private data is protected, and that Apple did not in fact screen iDevice Apps to prevent the dissemination of Apps that access personal information or invade users' privacy;

ix) That Apple did not in fact take the represented precautions to protect personal information on users' iDevices; and

x) That Apple did not in fact adequately fix security issues that allowed improper access to users' private information on iDevices, including address books.

304. The foregoing omissions were materially misleading.

305. Plaintiffs and class members relied upon the foregoing unlawful and fraudulent business acts and practices, including the foregoing material representations and omissions, to their detriment in that they overpaid for their iDevices, and would not have purchased the iDevices for the retail price paid had they known of the true facts.

306. As a result of the foregoing, each Plaintiff and class member has suffered harm.

307. Plaintiffs and class members relied upon the foregoing material representations and omissions to their detriment in that they overpaid for their iDevices, and would not have purchased the iDevices for the retail price paid or at all had they known of the true facts.

308. As a result of the foregoing, each Plaintiff and class member has been injured in fact, and has lost money or property, and each is entitled to restitution and injunctive relief.

309. Wherefore, Plaintiffs pray for relief and judgment as set forth below.

Count Six
Violations of the Unfair Competition Law (UCL)
California Business and Professions Code, § 17200 *et seq.*
(Against Apple on Behalf of All Plaintiffs)

310. Each Plaintiff, on his or her own behalf and on behalf of all class members, incorporates the above allegations by reference as if fully set forth herein, and further alleges as follows:

311. By its actions described in this complaint, Defendants have committed unlawful and fraudulent practices in violation of California Business & Professions Code section 17200 *et seq.* (the "UCL").

312. As a result of such actions, Plaintiffs and class members have suffered injury, and have lost money and property, including the inflated purchase price of their iDevices and their property in their mobile address books.

313. All Defendants engaged in unlawful business acts and practices in violation of the UCL by, among other things:

i) Invading Plaintiffs' and class members' privacy, as described above in Count One.

ii) Converting Plaintiffs' and class members' property, as describe above in Count Two.

314. In addition, Apple engaged in unlawful business acts and practices in violation of the UCL by, among other things:

i) Violating the FAL, as described above in Count Three;

ii) Violating the CLRA, as described above in Count Four;

iii) Violating California Civil Code section 1709 *et seq.*, as described in Count Five.

315. Apple engaged in fraudulent acts and practices in violation of the UCL, including by making the following misrepresentations:

i) Falsely and misleadingly representing that iDevices, and the information contained on iDevices, were safe and secure;

ii) Falsely and misleadingly representing that information contained in iDevices could not be accessed by others;

iii) Falsely and misleadingly representing that iDevice address books could not be accessed or collected by other Apps without the user's express permission;

iv) Falsely and misleadingly representing that it Apple gave users clear notice

and control over the information contained in their iDevices, including mobile contact book data;

v) Falsely and misleadingly representing that the iDevices, including their operating system, protected users from privacy attacks;

vi) Falsely and misleadingly representing that the iDevice, and its operating system, "sandboxed" data, including Contacts information and users' private address books, thereby preventing other Apps from accessing that data;

vii) Falsely and misleadingly representing that Apple protected the security of personal information and other data on the iPhone;

viii) Falsely and misleadingly representing that Apple subjected Apps to an approval process that ensured that users' private data is protected, and that Apple screens iDevice Apps to prevent the dissemination of Apps that access personal information or invade users' privacy;

ix) Falsely and misleadingly representing that Apple takes precautions to protect personal information on users' iDevices; and

x) Falsely and misleadingly representing that Apple fixed security issues that allowed improper access to users' private information on iDevices, including address books.

316. The foregoing representations were materially misleading. At the time that Apple made the foregoing representations, Apple did not believe they were true, or had no reasonable grounds for believing they were true.

317. Apple engaged in fraudulent acts and practices in violation of the UCL by its failure to disclose material facts that it was obligated to disclose because (a) Apple had exclusive knowledge of those material facts that were not known or reasonably accessible to Plaintiffs, the class, and the public; (b) Apple actively concealed those material facts from Plaintiffs, the class, and the public; and (c) the above representations by Apple, even if not deemed misrepresentations giving rise to independent liability, were partial representations that are

misleading because those other material fact has not been disclosed. The material facts not disclosed by Apple in violation of the UCL include:

i) That iDevices, and the information contained on iDevices, were not in fact safe and secure as represented;

ii) That information contained in iDevices could in fact be accessed by others;

iii) That iDevice address books could in fact be accessed or collected by other Apps without the user's express permission;

iv) That Apple gave users clear notice and control over the information contained in their iDevices, including mobile contact book data;

v) That the iDevices, including their operating system, ded not in fact protect users from privacy attacks;

vi) That the iDevice, and its operating system, ded not in fact "sandbox" data, including Contacts information and users' private mobile address books, and did not prevent other Apps from accessing that data;

vii) That Apple did not in fact protect the security of personal information and other data on the iPhone;

viii) That Apple did not in fact subject Apps to an approval process that ensures that users' private data is protected, and that Apple did not in fact screen iDevice Apps to prevent the dissemination of Apps that accessed personal information or invade users' privacy;

ix) That Apple did not in fact take the represented precautions to protect personal information on users' iDevices; and

x) That Apple did not in fact adequately fix security issues that allowed improper access to users' private information on iDevices, including address books.

318. The foregoing omissions were materially misleading.

319. Plaintiffs and class members relied upon the foregoing unlawful and fraudulent

business acts and practices, including the foregoing material representations and omissions, to their detriment in that they overpaid for their iDevices, and would not have purchased the iDevices for the retail price paid had they known of the true facts.

320. As a result of the foregoing, each Plaintiff and class member has suffered harm.

321. Plaintiffs and class members relied upon the foregoing material representations and omissions to their detriment in that they overpaid for their iDevices, and would not have purchased the iDevices for the retail price paid had they known of the true facts.

322. As a result of the foregoing, each Plaintiff and class member has been injured in fact, and has lost money or property, and each is entitled to restitution and injunctive relief.

323. Wherefore, Plaintiffs pray for relief and judgment as set forth below.

DEMAND FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and on behalf of the members of the Class defined herein, as applicable, pray for judgment and relief as follows as appropriate for the above causes of action:

A. An order certifying this case as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. An order that Defendants be enjoined from their improper activities and practices described herein, including but not limited to the following:

(1) That Apple immediately cease its unlawful, unfair and/or fraudulent business acts and/or practices and false and misleading advertising complained of herein;

(2) That Apple refrain from the false and misleading statements, and disclosing all material facts they were required to disclose, as described herein;

(3) That the App Defendants destroy and/or return to Plaintiffs and class members all information improperly obtained; and

(4) That Defendants refrain from any continued non-authorized use of the information of Plaintiffs and class members that was improperly obtained.

C. A judgment awarding Plaintiffs and class members actual, compensatory, statutory, presumed, punitive and/or exemplary damages, as appropriate for the particular Causes of Action;

D. A judgment granting declaratory relief, as appropriate for the particular Causes of Action;

E. A judgment awarding Plaintiffs and class members restitution for the unlawful, unfair and/or fraudulent business acts and/or practices and false and misleading advertising complained of herein; and requiring disgorgement of Defendants' unjust enrichment, wrongful profit or ill-gotten gains by requiring the payment of restitution to Plaintiffs and class members, as appropriate for the particular Causes of Action;

F. A judgment imposing on Defendants constructive trusts, as appropriate for the particular Causes of Action over any benefits wrongfully received or obtained by the Defendants or proceeds thereof;

G. Reasonable attorneys' fees, including but not limited to fees pursuant to California Code of Civil Procedure section1021.5 and California Civil Code section 1780(d);

H. All related costs of this suit;

I. Pre- and post-judgment interest; and

J. Such other and further relief as the Court may deem just, necessary, or appropriate.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims and issues herein.

Respectfully submitted,

Dated: June 27, 2014

KERR & WAGSTAFFE LLP

By: */s/ Michael Ng*
James M. Wagstaffe
Michael von Loewenfeldt
Michael Ng
KERR & WAGSTAFFE LLP

101 Mission Street, 18th Floor
San Francisco, CA 94105
Tel.: 415-371-8500
Fax: 415-371-0500
wagstaffe@kerrwagstaffe.com
mvl@kerrwagstaffe.com
mng@kerrwagstaffe.com

David M. Given
Nicholas A. Carlin
PHILLIPS, ERLEWINE & GIVEN LLP
50 California Street, 32nd Floor
San Francisco, CA 94111
Tel: 415-398-0900
Fax: 415-398-0911
dmg@phillaw.com
nac@phillaw.com

Interim Co-Lead Counsel for Plaintiffs

Carl F. Schwenker (admitted *pro hac vice*)
LAW OFFICES OF CARL F. SCHWENKER
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Tel: 512-480-8427
Fax: 512-857-1294
cfslaw@swbell.net

Plaintiffs' Liaison Counsel

Jeff Edwards (admitted *pro hac vice*)
EDWARDS LAW
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Tel: 512-623-7727
Fax: 512-623-7729
cfslaw@swbell.net

Jennifer Sarnelli
Kira German (admitted *pro hac vice*)
GARDY & NOTIS, LLP
501 Fifth Avenue, Suite 1408
New York, NY 10017
Tel: 212-905-0509
Fax: 212-905-0508
jsarnelli@gardylaw.com
kgerman@gardylaw.com

ATTORNEYS FOR PLAINTIFFS